TERRORISM AND DIGITAL FINANCING: HOW TECHNOLOGY IS CHANGING THE THREAT

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

JULY 22, 2021

Serial No. 117–25

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
45–867 PDF WASHINGTON : 2021

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
DONALD M. PAYNE, JR., New Jersey
J. LUIS CORREA, California
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
ERIC SWALWELL, California
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California
JOSH GOTTHEIMER, New Jersey
ELAINE G. LURIA, Virginia
TOM MALINOWSKI, New Jersey
RITCHIE TORRES, New York
JOHN KATKO, New York
MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, New Jersey
RALPH NORMAN, South Carolina
MARIANNETTE MILLER-MEEKS, Iowa
DIANA HARSHBARGER, Tennessee
ANDREW S. CLYDE, Georgia
CARLOS A. GIMENEZ, Florida
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
KAT CAMMACK, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York

HOPE GOINS, *Staff Director*
DANIEL KROESE, *Minority Staff Director*
NATALIE NIXON, *Committee Clerk*

SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM

ELISSA SLOTKIN, Michigan, *Chairwoman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
ERIC SWALWELL, California
JOSH GOTTHEIMER, New Jersey
TOM MALINOWSKI, New Jersey
BENNIE G. THOMPSON, Mississippi *(ex officio)*
AUGUST PFLUGER, Texas, *Ranking Member*
MICHAEL GUEST, Mississippi
JEFFERSON VAN DREW, New Jersey
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
JOHN KATKO, New York *(ex officio)*

BRITTANY CARR, *Subcommittee Staff Director*
ADRIENNE SPERO, *Minority Subcommittee Staff Director*
JOY ZIEH, *Subcommittee Clerk*

CONTENTS

TERRORISM AND DIGITAL FINANCING: HOW TECHNOLOGY IS CHANGING THE THREAT

Thursday, July 22, 2021

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE
AND COUNTERTERRORISM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:03 a.m., in room 310, Cannon House Office Building, Hon. Elissa Slotkin [Chairwoman of the subcommittee] presiding.

Present: Representatives Slotkin, Jackson Lee, Swalwell, Gottheimer, Malinowski, Thompson (ex officio), Pfluger, Guest, Van Drew, LaTurner, and Meijer.

Ms. SLOTKIN. The Subcommittee on Intelligence and Counterterrorism will come to order.

The subcommittee is meeting today on "Terrorism and Digital Financing: How Technology Is Changing the Threat."

Without objection, the Chair is authorized to declare the subcommittee in recess at any point.

Good morning, everyone. I want to thank our witnesses from the Department of Homeland Security for being here today to discuss a topic that I think is really timely and really interesting, which is how digital financial tools can be exploited by terrorist actors to funnel support for their activities.

Over the past several months, the abuse of digital finance platforms and technologies has jumped into the public view as the result of the burst of ransomware attacks that has struck the heart of day-to-day life in America, from gas pipelines and meat-processing plants to schools and hospitals.

Last month, just as an anecdote, I held an event in my district with the Secretary of Agriculture focused on small family farms. This was just days after the ransomware attack on the world's largest meat processor. I am in a room full of farmers. We are in the barn. There is the John Deere tractors behind us. When we opened it up to Q&A, the first question from the farmers was about cyber attacks, cryptocurrency, and asking what their Government was doing to protect them.

Now, let's be clear, there is nothing inherently illicit or illegal about cryptocurrencies or other digital finance technologies. They are used by millions of law-abiding people every single day. Nor is there anything inherently suspect about using technologies that aim to protect the privacy of users.

But it is our responsibility on this committee to also understand how these tools could enable malicious activity that threatens our homeland security, whether it is a ransomware like the one I discussed with those farmers or our topic today, funding for terrorism.

Detecting and preventing terrorist funding at home or abroad has long been a cat-and-mouse game for the Federal investigators in the intelligence community. Just like cyber criminals, terrorists consistently seek legal loopholes, illegal pathways, and new tech to stay one step ahead of governments, especially when it comes to funding their operations.

As a former CIA analyst, I know this is far from a new challenge. We have been tracking terrorist financing for decades, and I know first-hand how difficult it can be.

While the technology has changed, today's terrorists and extremist groups benefit from using many of the same tools that so many of us rely on for our daily, honest activities, just as they exploited commonly-used financial systems in the past.

Some of the on-line platforms and on-line tech allow easy access for thousands, if not millions, of users to donate money through on-line campaigns. For example, crowdfunding through PayPal, GoFundMe, and Amazon have become popular ways in recent years for extremist groups to raise money. Bitcoin has been the currency of choice for ransomware and terrorist actors.

To put this in context, according to the Global Project Against Hate and Extremism, from about 2005 to 2015, just about every extremist group they tracked featured a PayPal button on their website.

Now, even though PayPal and other payment-processing platforms became aware of the issue and began to ban extremists from their platforms, which is a great first step, these groups have persevered and maintained a strong on-line presence.

So, beyond social media platforms, new tech like cryptocurrencies, which are decentralized, largely anonymous forms of digital money, have enabled terrorists to further expand and disguise their funding efforts.

Think about, for many of us who were, sort-of, in the 9/11 era, the hawalas that we all became familiar with after 9/11, except now the currency is virtual instead of being filtered through couriers.

As these technologies become more and more widely used, we have seen a number of incidents in the past year that highlight the need for the Federal Government to understand these technologies, the degree to which they pose a threat, and their impact on terrorist financing.

There is a number of examples from recent weeks; I am sure you all will be talking about them. But just as nefarious groups have changed their fundraising tactics after crackdowns by payment processors like PayPal, when law enforcement begins following and cracking down on illicit Bitcoin use, terrorist fundraisers advise supporters to use other cryptocurrencies to avoid detection. This was the case of a pro-ISIS website that requested its supporters send money via Monero, another cryptocurrency, instead of Bitcoin, because of its privacy and safety features.

So we just need to properly understand and combat this threat. We know that it requires a lot of partnership between the private sector, our allies and partners—and, of course, a task the Department of Homeland Security is well-positioned to lead.

I will just end by saying, today, I am hoping our witnesses will help us understand the actual scope and scale of this challenge. How much money are we talking about? How does it compare to terrorist financing as a whole or the total amount of cryptocurrency transactions? Who is taking advantage of this new tool? Is it domestic or foreign groups? Just help us contextualize a little bit.

We know we have an uphill battle. Our subcommittee stands ready to help the Department with what you need. If you need changes to legislation, if you need resources, we want to hear more from you, not less.

So we are pleased to welcome our witnesses today.

I will just note that, as I mentioned to the witnesses, we expect votes to be called probably in the next 10 minutes. We will try and keep the hearing going as long as possible. There will probably be a short gap when myself and Mr. Malinowski are voting, but we will try to tag-team to make it as minimal as possible.

[The statement of Chairwoman Slotkin follows:]

STATEMENT OF CHAIRWOMAN ELISSA SLOTKIN

JULY 22, 2021

Over the past several months, the abuse of digital finance platforms and technologies has jumped into public view, as a result of the burst of ransomware attacks that have struck at the heart of day-to-day life in America—from pipelines and meat processing plants, to schools and hospitals. Last month, I held an event in my district with the Secretary of Agriculture that was focused on family farms—just days after a ransomware attack on the world's largest meat processor. And in a room full of Michigan farmers, the first question was about cryptocurrency—asking what our Government can do to track and recover digital payments of ransoms to these criminal groups.

Now, let's be clear: There's nothing inherently illicit or illegal about cryptocurrencies or other digital finance technologies, which are used by millions of law-abiding people every day. Nor is there anything inherently suspect about using technologies that aim to protect the privacy of users. But it's our responsibility on this committee to also understand how these tools could enable malicious activity, that threatens our homeland security—whether that's a ransomware attack, like the one I discussed with those farmers, or our topic today: Funding for terrorism. Detecting and preventing terrorist funding—at home, and abroad—has long been a cat-and-mouse game for Federal investigators and the intelligence community.

Just like cyber criminals, terrorists consistently seek legal loopholes, illegal pathways, and new technologies to stay one step ahead of governments—especially when it comes to funding their operations. As a former CIA analyst, I know this is far from a new challenge—we've been tracking terrorist financing for decades—and I know first-hand how difficult it can be. While technology has changed, today's terrorist and extremist groups benefit from using many of the same tools that so many of us rely on for our daily, honest activities—just as they exploited commonly-used financial systems, in the past. Some of these on-line platforms and on-line technologies allow easy access for thousands—if not millions—of users to donate money through on-line campaigns. For example, crowdfunding through PayPal, GoFundMe, and Amazon became a popular way in recent years for extremist groups to raise money. To put this into context, according to the Global Project Against Hate and Extremism, from about 2005–2015, just about every extremist group they tracked featured a PayPal button on their website.

Now, even though PayPal and other payment processing platforms became aware of the issue and began to ban extremists from such platforms—at first glance, a promising first step—extremist and terrorist groups have persevered and maintained an on-line presence. For example, ISIS supporters have recently used Instagram to solicit donations for ISIS-affiliated women being detained in Syria, via

PayPal fundraising links. Beyond social media platforms, new financial technologies like cryptocurrencies—which are decentralized, largely anonymous forms of digital money—have enabled terrorists to further expand and disguise their funding efforts.

As these technologies become more and more widely used, we've seen a number of incidents just in the past year that highlight the need for the Federal Government to understand these technologies, the degree to which they pose a threat, and their impact on terrorist financing. In August 2020, the Justice Department "dismantle[ed] three terrorist financing cyber-enabled campaigns" involving Foreign Terrorist Organizations (FTOs)—ISIS, Hamas' military wing, and al-Qaeda—resulting in the Government's largest-ever seizure of cryptocurrency from terrorist organizations. The seizure involved "millions of dollars" spanning 300 cryptocurrency accounts, four websites, and four Facebook pages—underscoring how various digital technologies could be used to help foster fundraising efforts.

Just as nefarious groups changed fundraising tactics after crackdowns by payment processors like PayPal, when law enforcement began following and cracking down on illicit Bitcoin use, terrorist fundraisers advised supporters to use other cryptocurrencies, to avoid detection. This was the case with a pro-ISIS website that requested that its supporters send money via Monero, another cryptocurrency, instead of Bitcoin, because of its privacy and safety features. Properly understanding and effectively combating this threat will require close partnerships between all levels of government, the private sector, and our allies—a task the Department of Homeland Security is well-positioned to lead.

Today, I'm hoping our witnesses can help us understand the actual scope and scale of this challenge:

- How much money are we talking about?
- How does it compare to terrorist financing as a whole, or the total amount of cryptocurrency transactions?
- Who's taking advantage of it: Domestic or foreign groups?

I'm also interested in understanding how the intelligence and law enforcement approach to illicit digital financing compares to your historical work on terrorist funding, and the steps you're taking to combat it. It's clear that our law enforcement and intelligence community face an uphill battle in understanding and tackling this threat—as the examples I've outlined show, the technology is changing rapidly, as their adoption only continues to increase.

Our subcommittee stands ready to help the Department take on this challenge, and we're pleased to welcome our witnesses today. I look forward to hearing from you about the trends the Department is currently monitoring on this issue and the novel ways it is working to counter terrorists' use of digital financing.

Ms. SLOTKIN. So I now recognize the Ranking Member of the subcommittee, the gentleman from Texas, Mr. Pfluger, for an opening statement.

Mr. PFLUGER. Thank you, Madam Chair. I appreciate you holding this hearing today.

I would like to thank the witnesses as well: Assistant Director Jeremy Sheridan from the Office of Investigations at the Secret Service, Assistant Director John Eisert from Investigative Programs at HSI, and Acting Deputy Under Secretary Stephanie Dobitsch from the Office of Intelligence and Analysis.

I appreciate your expertise and your willingness to speak with us today on this very important subject. I am looking forward to an informative and productive discussion on this very important topic.

I think this hearing is especially timely right now, with American troops, in effect, fully withdrawn from Afghanistan and the Taliban rapidly taking control of Afghanistan's provincial districts, reportedly occupying about a third of the country and including the key border-crossing areas.

Afghan Security Forces are surrendering. The Taliban is beginning to fight for some of the provincial cities. There is reporting, public reporting, that the Afghan government could collapse at some point, as soon as maybe even 6 months.

But I think the point is, all that to say that foreign terrorist organizations are alive and well. Not only are they present overseas, but they are growing. As we know, Afghanistan is only a portion of the wide-spread and diverse terror threat landscape that we face around the world. If they are given the opportunity to submit their presence overseas, I have no doubt that their next goal is and will continue to be to launch an attack on U.S. soil or on those of our partners and allies.

Those who have served in Afghanistan saw first-hand the death and destruction that terrorist organizations can cause and have caused. It is absolutely imperative that the war on terror be fought abroad, on foreign soil, not here at home. We must guarantee that foreign terrorist organizations do not have the resources to expand their operations and bring the fight to the United States, to our homeland.

Cutting off their access to financing is absolutely critical. It is paramount in this fight. Terrorist financing is not a new issue. Whether a transnational criminal organization, a foreign terrorist organization, or money launderer, we have been confronting this problem for decades. But cryptocurrency is, in fact, becoming a new tool that terrorists and other criminal enterprises have at their disposal.

Unfortunately, Congress has not always been known for our ability to stay one step ahead, when it comes to the latest technological advances. But, when we are confronting the issue of terrorism and financing, playing catch-up is not an option for us.

During a conversation I had earlier this week with Assistant Director Sheridan and Assistant Director Eisert, they mentioned that, relative to the terrorist-financing world, that cryptocurrency and the transactions account for maybe 1 percent of all cases.

I think that this tells me right now that we are having this hearing at exactly the right time, that we might have a chance to stay one step ahead of what the issues and the problems could be, before this becomes a systemic issue world-wide. We are now in a position to provide our agency partners with the resources and the authorities that they need to confront this proactively instead of reacting to it.

That is why I am most looking forward to the hearing—about the hearing today. How do we ensure that cryptocurrency transactions continue to be 1 percent, or maybe even less, of the problem? What does DHS need from us in Congress to best situate themselves to combat this threat?

Coming out of this hearing, I also hope to understand what we should expect going forward. Although this is a small portion of the problem now, do we foresee that changing? If it is suspected to grow, how much will it grow, and how can we minimize that growth?

It has been almost 20 years since 19 al-Qaeda terrorists coordinated the hijacking of 4 commercial airlines, flying them into buildings which were recognized world-wide as symbols of American strength, of freedom, of accomplishment, and taking 2,977 innocent lives.

Thus far, we have successfully prevented an attack of that magnitude that we experienced on September 11. As long as I serve my

country—and I think the Chairwoman will also agree—whether it is in uniform overseas or in the capacity that we now serve here in Congress, I will do everything and I think I can confidently say we will do everything in our power to ensure that what happened on 9/11 does not happen again. I am confident that my fellow Members on the Homeland Security Committee also feel the same way in a very bipartisan manner.

I am looking forward to working with Chairwoman Slotkin and the other Members of this committee to ensure that we are providing the Department with all the tools necessary to minimize the threat caused by terrorist financing and to successfully protect our homeland.

Once again, I would like to thank our witnesses for joining us today, for your expertise, for your service to this country, and for looking at a threat in a proactive way that we can combat now so that it doesn't continue to become a problem of larger magnitude.

With that, Madam Chair, I yield back.

[The statement of Ranking Member Pfluger follows:]

STATEMENT OF RANKING MEMBER AUGUST PFLUGER

Thank you, Madam Chair. I appreciate you holding this hearing today and thank our witnesses: Assistant Director Jeremy Sheridan from the Office of Investigations at the Secret Service, Assistant Director John Eisert from Investigative Programs at HSI, and Acting Deputy Under Secretary Stephanie Dobitsch from the Office of Intelligence and Analysis. I am looking forward to an informative and productive discussion on this very important topic.

This hearing is especially timely, with American troops in effect fully withdrawn from Afghanistan, and the Taliban rapidly taking control of Afghanistan's provincial districts—reportedly occupying about a third of the country including key border-crossing areas. Afghan security forces are surrendering, and the Taliban is beginning to fight for some of the provincial cities. There has been public reporting that the Afghan government could collapse within 6 months of our withdraw. All this to say that foreign terrorist organizations are alive and well. Not only are they present overseas, but they are growing, and as we all know Afghanistan is only a portion of the wide-spread and diverse terror threat landscape. If they are given the opportunity to cement their presence overseas, I have no doubt that their next goal will be to launch an attack on U.S. soil.

Those who served in Afghanistan saw first-hand the death and destruction that terrorist organizations cause. It is absolutely imperative that the war on terror be fought on foreign soil. We must guarantee that foreign terrorist organizations do not have the resources to expand their operations and bring the fight to the homeland. Cutting off their access to financing is absolutely critical.

Terrorist financing is not a new issue. Whether a transnational criminal organization, foreign terrorist organization, or money launderer, we have been confronting this problem for decades. But crypto currency is a new tool that terrorists and other criminal enterprises have at their disposal. Unfortunately, Congress has not always been known for our ability to stay one step ahead when it comes to the latest technological advances, but when we're confronting the issue of terrorism financing, playing catch-up is not an option. During a conversation I had earlier this week with Assistant Director Sheridan and Assistant Director Eisert, they mentioned that relative to the entire terrorist financing world, crypto currency transactions account for about 1 percent of cases. That tells me we are having this hearing at exactly the right time—before this is a systemic problem. We are now in the position to provide our agency partners with the resources and authorities they need to confront this proactively, as opposed to reactively.

That is what I am most looking forward to hearing about today—how do we ensure that crypto currency transactions continue to be 1 percent of the problem. And what does DHS need from us in Congress to best situate themselves to combat this threat?

Coming out of this hearing I also hope to understand what we should expect going forward. Although this is a small portion of the problem now, do we foresee that changing? If it is suspected to grow—how much and how can we minimize any growth?

It has been almost 20 years since 19 al-Qaeda terrorists coordinated the hijacking of four commercial airlines, flying them into buildings which were recognized worldwide as symbols of American strength and accomplishment, taking 2,977 innocent lives. Thus far we have successfully prevented an attack of the magnitude we experienced on September 11. As long as I serve my country, whether in uniform overseas or here in Congress, I will do everything in my power to ensure that what happened on 9/11 does not happen again and I am confident that my fellow Members on the Homeland Security Committee feel the same way.

I am looking forward to working with Chairwoman Slotkin and the other Members of the subcommittee to ensure that we are providing the Department with all of the tools necessary to minimize the threat caused by terrorist financing and successfully protect the homeland.

I thank our witnesses for their willingness to appear before the subcommittee, today, and I yield back the balance of my time.

Ms. SLOTKIN. Additional Member statements will be submitted for the record.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

JULY 22, 2021

We are here today to talk about the use of modern financial technologies for terrorist fundraising and financing. The mantra "follow the money" has been one of the most effective ways of investigating and stopping criminal and terrorist activity. But since this committee was formed after 9/11, we have seen the rise of new platforms like Paypal and GoFundMe and entirely new types of money developed in the form of cryptocurrencies. These financial technologies and the digital marketplaces that make use of them have revolutionized the American economy and global markets.

Unfortunately, they have complicated law enforcement and intelligence community efforts to detect and prohibit terrorist financing. As Treasury Secretary Janet Yellen told the Senate Finance Committee, cryptocurrencies "can be used to finance terrorism, facilitate money laundering, and support malign activities that threaten U.S. national security interests. . . ."

Following the money is undoubtedly a different task than it was at the outset of the War on Terror. Yet, it remains a crucial guidepost in our efforts to root out terrorists and strengthen National security. We must ensure that our intelligence and law enforcement agencies have the tools and capabilities to keep pace with technological changes and new terrorist financing practices.

I was pleased to support Rep. Kathleen Rice's bill, the Homeland Security Assessment of Terrorists' Use of Virtual Currencies Act, which required the Department of Homeland Security to produce a threat assessment of terrorists' use of virtual currency. And I look forward to hearing how this assessment has informed the Department's efforts to combat such activity.

I am pleased that Chairwoman Slotkin is leading on this critical issue by holding today's hearing. I look forward to a productive conversation on this topic and to working with DHS, its components, and interagency partners to ensure they have the resources they need.

Ms. SLOTKIN. I now welcome our panel of witnesses.

Our first witness is Ms. Stephanie Dobitsch, the deputy under secretary for intelligence enterprise operations at DHS. Our second witness is Mr. John Eisert, the assistant director of investigative programs at U.S. Immigration and Customs Enforcement, Homeland Security Investigations, HSI. Our third and final witness is Mr. Jeremy Sheridan, the assistant director of the Office of Investigations at the U.S. Secret Service.

Without objection, the witnesses' full statements will be inserted into the record.

I now ask each witness to summarize his or her statement for 5 minutes, beginning with Deputy Under Secretary Dobitsch.

STATEMENT OF STEPHANIE DOBITSCH, DEPUTY UNDER SECRETARY, OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY

Ms. DOBITSCH. Good morning, Chairwoman Slotkin, Ranking Member Pfluger, Members of the subcommittee. Thank you for the opportunity to appear before you today to represent the Office of Intelligence and Analysis and to discuss the malicious use of crypto and other digital currencies.

Over the last several years, I&A has observed a growing and concerning trend of a wide range of malicious actors seeking to use access to digital and cryptocurrencies to facilitate their activities. This includes domestic and international terrorists, nation-state adversaries, transnational and other criminal organizations, and cyber criminals.

While the intent and capabilities of these actors vary widely, I&A assesses that all of them see using crypto and other digital currencies as an effective means to obfuscate and fund their operations, including against the United States.

Cryptocurrencies are a digital or virtual currency that is secured by cryptography, or, in other words, sophisticated coding. They are not issued by any central authority, and they offer users a high degree of anonymity, complicating law enforcement and intelligence community efforts to identify and disrupt potentially threatening activity.

Bitcoin is the market leader, but there are thousands of other cryptocurrencies, including currency known as privacy coins, which provide an even greater level of obscurity for malicious actors. This means that users can easily hide who is sending or receiving a transaction, transaction amounts, and individual units of currency.

Since at least 2015, we have observed terrorists seeking to use cryptocurrencies to procure materials and solicit funding for their operations. Most of this activity has occurred by terrorist groups and associates overseas, spanning the ideological spectrum. For example, supporters of ISIS and al-Qaeda have solicited cryptocurrency donations. Earlier this year, a pro-al-Qaeda media group offered a reward of 1 Bitcoin, worth about $60,000 at the time, to the first person to kill a police officer in a Western country.

We have also seen foreign racially- or ethnically-motivated violent extremists claim that their activities were supported by the use of cryptocurrencies. In 2019, Brenton Tarrant, the perpetrator of the mosque attacks in Christchurch, New Zealand, claimed in his manifesto to have made money dealing in cryptocurrency. Later that same year, a racially- or ethnically-motivated violent extremist who attempted an attack in a synagogue in Germany claimed he received financial support for his operation via cryptocurrency.

Beyond terrorism, the use of cryptocurrency has become even more common among cyber actors and criminal organizations. North Korean cyber actors affiliated with the regime have executed lucrative cryptocurrency thefts valued at hundreds of millions of dollars. Cryptocurrency is increasingly being used to buy and sell drugs on the dark web and by drug cartels seeking to launder their drug profits. Cryptocurrency is becoming the payment of choice for cyber criminals who are conducting ransomware attacks or selling malicious cyber services on-line.

It is important to remember that the illicit use of cryptocurrency is a small fraction of the global transactions that occur daily, and many malicious actors, particularly foreign terrorist groups, are still relying on traditional means of funding.

However, as this technology becomes more accessible and more scrutiny is applied to traditional banking systems, we expect to see more activity, and our ability to detect and disrupt these threat actors will be even more difficult.

I&A's mandate and core mission is to provide Federal, State, local, Tribal, territorial, and private-sector partners with the intelligence and information necessary to secure the homeland. I want to underscore that I&A is committed to strengthening our efforts to identify and communicate the plans and intentions of malicious actors seeking to exploit emerging technologies like cryptocurrency.

Just this week, I&A hosted our partners from the State and local intelligence councils for a conference, where this topic was discussed as a significant intelligence gap in our intelligence.

Like with any threat to the homeland, I&A will ensure that policy and operational decision makers have the most robust understanding of this threat that the intelligence community can provide.

Thank you again for the opportunity to appear before you today to discuss this issue and for your continued support to the Office of Intelligence and Analysis.

[The prepared statement of Ms. Dobitsch follows:]

PREPARED STATEMENT OF STEPHANIE DOBITSCH

JULY 22, 2021

Chairwoman Slotkin, Ranking Member Pfluger, and distinguished Members of the Subcommittee on Intelligence & Counterterrorism. Thank you for the opportunity to appear before you today to discuss threats from terrorist use of cryptocurrencies. It is an honor to be here representing the Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A), and the dedicated intelligence professionals that keep the homeland safe, secure, and resilient.

TERRORIST USE OF CRYPTOCURRENCY

As we have learned in our fight against terrorism, terrorists are highly adaptive and have proven successful in exploiting new and emerging technologies to plan attacks against U.S. interests and the homeland. While some of those technologies, such as drones and 3D printing, pose direct harm, it is often access to sources of funding that are difficult to trace or attribute that allow terrorist groups even greater means to conduct a broad range of operations against the United States. Additionally, as governments and the global financial industry devote more resources to restricting terrorist use of traditional banking systems, the relative ease and anonymity of cryptocurrencies are helping to offset these restrictions, including for other malicious actors seeking to do harm to the United States.

Since at least 2015, we have observed terrorists experimenting with cryptocurrencies to obfuscate their financial activities, procure materials, and solicit donations for their operations. These activities have spanned the spectrum of terrorist ideologies—from Racially or Ethnically Motivated Violent Extremists (RMVEs), to groups like the Islamic State of Iraq and ash-Sham (ISIS), al-Qaeda, and HAMAS. Using cryptocurrencies may be attractive to terrorists and supporters of violent extremism because they appear to offer a level of anonymity and less government oversight.

We have seen ISIS supporters around the world requesting donations in cryptocurrency and they may have used the donated cryptocurrency to purchase website domains in 2015 and 2018. Since at least 2018, other individuals who support violent extremism abroad, as well as individuals who support RMVE ideologies, have solicited multiple types of cryptocurrency from on-line donors via social media.

Also, receiving payments through cryptocurrency has risen in popularity, especially among Racially or Ethnically Motivated Violent Extremists (RMVE). For example, in March, the FBI arrested a RMVE on a weapons charge who sold merchandise via social media platforms and accepted payment in a variety of ways, including cryptocurrency. Additionally, in June a pro-al-Qaeda media group overseas offered a reward of one Bitcoin—which was worth around $60,000 at the time—to the first person to kill a police officer in a Western country in response to the announcement.

To date, we are not aware of any specific cases where Domestic Violent Extremists (DVEs) or Home-grown Violent Extremists (HVEs) in the homeland have leveraged cryptocurrency to directly fund an attack. A review of DVE and HVE violence in the United States reveals that most attacks involved simple, easy to acquire weapons that were personally financed.

There are a handful of examples of DVEs abroad utilizing cryptocurrency to facilitate violence, including a RMVE in Germany who attacked a synagogue in 2019 and received financial support for attack preparation from an unknown individual via cryptocurrency. Additionally, a RMVE attacked a mosque in Christchurch, New Zealand, and claimed in his manifesto to have made money dealing in cryptocurrency, however investigators assess he did not make significant profits. Regardless of what we have witnessed in the United States to date, we know that terrorists historically are adaptive and often seek to embrace new technologies, and activities overseas can often foreshadow developments domestically.

In addition to concerns about terrorists using existing cryptocurrency, we are also concerned about the speed and complexity in which cryptocurrencies develop and advance to improve the user experience, including increased privacy measures, which challenges our collective abilities in the U.S. Government to identify and mitigate malicious use of this technology. Bitcoin is the market leader of cryptocurrencies and, unsurprisingly, it is also the most popular cryptocurrency for criminal and terrorist use. However, newer and less popular cryptocurrencies, known as "privacy coins," are increasingly attractive to malicious actors because they include even more stringent privacy and security features. We already know that terrorists affiliated with ISIS, RMVEs, and other violent extremists are using these privacy coins to conduct financial activities while obfuscating their identies.

Finally, it is important to keep in mind that the vast majority of terrorist financing occurs through methods other than cryptocurrency, and most cryptocurrency is used legitimately. But cryptocurrency has some appealing attributes that have already been exploited by terrorists, and we anticipate violent extremists will continue to use this tool to facilitate their terrorist activities, especially as the technology becomes easier to access and more wide-spread in use in general commerce and the commercial sector. As these technologies become increasingly ubiquitous, the opportunity for malicious actors to exploit them will grow.

I&A EFFORTS

I&A's mandate and core mission is to provide our State, local, Tribal, territorial, and private-sector partners with the intelligence and information necessary to secure the homeland. This includes establishing and running analytic seminars on the illicit use of cryptocurrency and the dark web to inform our partners on the illicit use of the dark web, blockchain technology, major cryptocurrencies used, how criminals are using cryptocurrencies to launder money and make illegal transactions, and key tools and best practices that analysts can leverage in Dark Web and cryptocurrency investigations. And I want to underscore that I&A is committed to strengthening our efforts to identify and communicate threats from foreign and domestic terrorists, including their plans and intentions to exploit emerging technologies such as cryptocurrency through a number of recently-published pieces of Classified and un-Classified analytic production. I&A is also working to support our colleagues across DHS and the intelligence community through sharing and analyzing cryptocurrency data to enhance our understanding of the threat across the National security and law enforcement landscape. As with any threat to the homeland, we are committed to ensuring policy makers and operational decision makers have the most robust understanding of the threat that the intelligence community can provide.

CONCLUSION

Thank you again for the opportunity to appear before you today to discuss this critical threat and for your continued support for I&A. We remain committed to keeping the homeland safe, secure, and resilient by safeguarding the Nation from terrorist, criminal, and other threat actors; protecting the physical and digital borders of the United States from Transnational Criminal Organizations and terrorist

networks seeking to exploit and undermine our financial and cyber systems; and we will continue our efforts at home and abroad to uphold the National security and public safety of the United States.

Ms. SLOTKIN. Thank you, Ms. Dobitsch.

I now recognize Assistant Director Eisert to summarize his statement for 5 minutes.

My sense is we may break just after Mr. Eisert for a few moments while we go and vote.

STATEMENT OF JOHN EISERT, ASSISTANT DIRECTOR, INVESTIGATIVE PROGRAMS, HOMELAND SECURITY INVESTIGATIONS, IMMIGRATION AND CUSTOMS ENFORCEMENT, DEPARTMENT OF HOMELAND SECURITY

Mr. EISERT. Thank you, Chairwoman Slotkin, Ranking Member Pfluger, and distinguished Members of the subcommittee. Thank you for the opportunity to appear before you today to discuss the critical investigative role Homeland Security Investigations plays in the fight to protect the homeland from transnational crime and threats.

My testimony today will focus on HSI's efforts to identify, investigate, and bring to justice criminal organizations and terrorist networks whose illicit use of cryptocurrency jeopardizes National security and public safety.

As the principal investigative component of the Department of Homeland Security, HSI is a global law enforcement organization responsible for conducting criminal investigations into the illegal cross-border movement of goods, money, contraband, people, and technology into, out of, and throughout the United States.

HSI strives to protect the homeland's digital borders and pursue malicious cyber actors with the same dedication that we safeguard our physical land and sea borders. HSI applies its unique authorities and capabilities to conduct investigations, which include combating financial crime, investigating cyber crime, and protecting National security. The illicit use of cryptocurrency by nefarious actors leads to each of these priorities.

Cryptocurrency is a digital asset that works as a medium of exchange or a store of value and is often used to purchase illicit items such as drugs or guns on the dark net marketplaces, to launder criminally-derived proceeds, or as a means to provide material support to terrorist organizations. Traditional money-laundering methods remain, yet cryptocurrency can now be used with relative ease to facilitate any type of illicit activity.

Given that cryptocurrency is utilized across the spectrum of crimes that HSI has the authority to investigate, HSI plays a critical role in the U.S. Government's efforts to detect, investigate, and prevent its illicit use.

As such, HSI investigations related to cryptocurrency have risen from a single criminal investigation in 2011 to over 604 active criminal investigations and $80 million in cryptocurrency seizures in this year alone. This marked increase signifies growing confidence in cryptocurrency by bad actors but also HSI's technical proficiency in performing these complex investigations.

To be successful, HSI recognizes the importance of enhanced public and private partnerships. With that, we continue to be for-

ward-leaning in our approach to Operation Cornerstone, our outreach efforts.

Since 2019, HSI has provided 660 presentations to over 61,000 attendees, with the primary focus of detecting and closing vulnerabilities in the financial, trade, and transportation sectors. With the rapid growth of virtual currency, HSI expanded our outreach to include private industries involved in the cryptocurrency space, conducting 116 presentations to over 5,000 participants.

The relationship we build with private sector directly correlates to our investigative success. They are not mutually exclusive.

Last year, HSI led a global cyber operation with IRS and the FBI related to 24 cryptocurrency accounts, all of which were identified as sources of influence for al-Qaeda. The HSI undercover operation was initiated to investigate the unlawful use of cryptocurrency to support terrorism. The result of the investigation—ending result of the investigation, HSI seized 60 virtual currency wallets, worth $80 million, and illuminated the illicit financial network.

In another case, HSI initiated another cyber undercover operation that resulted in the seizure of 150 cryptocurrency accounts, worth $2 million, and the taking over of a Hamas-administered website that solicited funds for jihad. HSI covertly operated this site, embedding an HSI undercover wallet and email to track funds and communications.

The results of these cases and others illustrate how law enforcement can effectively disrupt terrorist groups through the use of HSI's financial and global investigative authorities, technical aptitude, undercover authorities, and the ability to use private sector as a force multiplier to disrupt and dismantle the command-and-control structure of these criminal organizations.

In closing, I appreciate your interest in this rapidly-growing field. Thank you again for the opportunity to be before you today and for your continued support of Homeland Security Investigations. Thank you.

[The prepared statement of Mr. Eisert follows:]

PREPARED STATEMENT OF JOHN EISERT

THURSDAY, JULY 22, 2021

INTRODUCTION

Chairwoman Slotkin, Ranking Member Pfluger, and distinguished Members: Thank you for the opportunity to appear before you to discuss the critical investigative role U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) plays in the fight to protect the homeland from transnational crime and other threats. My testimony today will focus on HSI's efforts to identify, investigate, and ultimately bring to justice criminal and terrorist organizations whose illicit use of cryptocurrency jeopardizes the National security and public safety of the United States.

THE HSI MISSION

As the largest investigative component of the Department of Homeland Security, HSI is the premier law enforcement organization responsible for conducting Federal criminal investigations into the illegal cross-border movement of goods, money, technology, people, and other contraband into, out of, and throughout the United States. HSI strives to protect the homeland's digital borders and pursue malicious cyber actors with the same dedication it safeguards our land and sea borders from traditional organized transnational crime.

HSI's operational priorities serve as the foundation of HSI's investigative and enforcement focus. HSI applies its unique authorities and capabilities to conduct complex and significant transnational investigations aligned with these priorities, which include combating financial crime, investigating cyber crime, and protecting National security. The illicit use of cryptocurrency by nefarious actors relates to each of these priorities and represents a key area of focus for HSI's investigations and operations.

HSI participates in and has representation on dozens of collaborative cyber-related efforts, including the HSI Cyber Crimes Center, the Federal Bureau of Investigation's National Cyber Investigative Joint Task Force, the U.S. Secret Service Electronic Crimes Task Force, and the DHS Science and Technology Internet Anonymity Project Working Group.

CRYPTOCURRENCY AND THE THREAT IT POSES TO THE HOMELAND

A cryptocurrency is a digital asset that works as a medium of exchange, a unit of account, or a store of value. Cryptocurrency uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. In 2009, Bitcoin was introduced as the first decentralized convertible virtual currency and offered a high level of pseudo-anonymity for people to send and receive money over the internet. While Bitcoin is by far the most popular and well-known cryptocurrency, thousands of cryptocurrencies have been created and new ones are created every day. There is open source or proprietary software that anyone can use to create a cryptocurrency.

Since 2009 cryptocurrencies have increasingly been used as the currency of choice to facilitate crime. From individual actors to large-scale transnational criminal organizations (TCOs), cryptocurrency can be exploited by any criminal organization engaged in almost any type of illicit activity. Cryptocurrencies are attractive to criminal and terrorist organizations because they offer a relatively fast, inexpensive, and pseudonymous system of transactions as compared to more traditional financial transactions.

HSI has seen that nefarious actors are inclined to use cryptocurrency based on the perception that there is anonymity associated with their transactions or that because cryptocurrency used during an illicit scheme can be moved immediately offshore to a foreign exchange or over the counter trader (OTC), that U.S. law enforcement entities will be unable to trace or to seize and recover the assets. In addition, cryptocurrency offers the ability to engage in money laundering with minimal effort. By using OTCs or offshore exchanges, cryptocurrency can be laundered and reintroduced into the U.S. financial system relatively easily by utilizing typical laundering techniques of placement and layering. When used to fund terrorist operations and activities, terrorist organizations often have the opposite requirement. They seek to conceal the origin of funds from donors, businesses, and other legitimate sources to avoid law enforcement scrutiny.

HSI has seen nefarious actors expend cryptocurrency in furtherance of a wide array of crimes HSI investigates. Both at home and abroad, cryptocurrency can be used to purchase illicit items such as drugs or guns on darknet marketplaces; to launder criminally-derived proceeds; or to provide material support to or funding for terrorist actors or organizations to carry out operations. Cryptocurrency can also be used to pay fraudsters, ransomware actors, or individuals involved in other illicit schemes such as intellectual property theft and illegal technology procurement. In addition, current trends indicate cryptocurrency is becoming prevalent within criminal organizations involved in child exploitation and human trafficking. Whether expended by TCOs, or terrorist organizations, or facilitators of such organizations, the use of cryptocurrency by bad actors continues to expand and evolve and presents a potential threat to the National security and public safety of the United States.

HSI'S LINES OF EFFORT

Given that cryptocurrency is used across the spectrum of crimes that HSI has the authority to investigate, HSI plays a critical role in the U.S. Government's efforts to detect, investigate, and prevent its illicit use by criminal and terrorist actors. Using its authorities and subject-matter expertise in financial, cyber, and National security cases; its strong strategic partnerships; and its robust international footprint, HSI employs a multi-faceted approach to combat crimes enabled by the use of cryptocurrency. This approach is rooted in HSI's investigative expertise, and supplemented by robust collaboration, training, and outreach programs. These efforts are described below.

Investigations

Bitcoin and other cryptocurrencies are attractive to bad actors because of their pseudo-anonymity and ease of transfer, but at some point, criminals need to convert their cash into cryptocurrency or their cryptocurrency into cash. Whenever monetary exchanges are made, a chokepoint is created. This is the time when criminals are most vulnerable and can be identified through law enforcement means and methods. Using traditional investigative methods such as surveillance, undercover operations, and confidential informants, coupled with sophisticated financial and blockchain analysis, HSI can take advantage of these chokepoints and use them to identify, disrupt, and dismantle the terrorist organizations and TCOs.

In 2013, the U.S. Department of the Treasury's Financial Crimes Enforcement Network issued guidance clarifying that certain persons or companies that exchange convertible virtual currency, such as cryptocurrency, are considered money services businesses (MSBs), and therefore must follow the same regulatory and reporting protocols as traditional MSBs. The protocols include developing and implementing an anti-money laundering compliance program, filing suspicious activity reports, and registration requirements, among others. These procedures include "Know Your Customer" measures to record personal identifying information from customers to mitigate fraud. Lawful users of cryptocurrencies tend to use registered, compliant cryptocurrency exchanges that adhere to regulatory and operational measures in exchange for security, low fees, and the ease of processing transactions.

Those who use cryptocurrency for illegal purposes generally avoid registered exchanges and seek illicit or unregistered exchanges that do not require or ask for personal identifying information. These illicit exchanges often take the form of a direct Peer-to-Peer (P2P) exchanger. P2P exchangers post advertisements stating the price for which they are willing to either buy or sell cryptocurrency on-line. Although some P2P exchangers do register with FinCEN and State authorities and follow compliance laws, most do not. Rather, these illicit P2P exchangers position themselves as the money launderers in the cryptocurrency world. P2P exchangers illegally generate revenue by charging a premium for allowing their customers to remain anonymous. They will sell cryptocurrency above market value and buy below market value to or from those customers who want to remain anonymous.

Targeting these illicit P2P exchangers enables HSI to open the door and pull back the veil of pseudo-anonymity provided by cryptocurrencies. HSI can identify other criminals using cryptocurrency to fund and further their illicit activities through interviews and suspect cooperation; forensic analysis of computers, mobile phones, and other seized electronics; and the use of advanced blockchain tracing tools.

Since 2018, HSI's Cryptocurrency Intelligence Program (CIP), housed at the National Bulk Cash Smuggling Center, has targeted unlicensed cryptocurrency MSBs and other gatekeepers in the cryptocurrency space. CIP provides blockchain forensics and analytics support to HSI investigators, as well as State, local, and international partners investigating cryptocurrency-enabled crimes. CIP uses technical and subject-matter expertise to exploit blockchain evidence, guide agency policy, monitor market intelligence, and regularly engages with private-sector partners such as exchanges, other virtual asset service providers and the blockchain industry groups.

Collaboration

With the rapid development of new technologies, TCOs and terrorist organizations often adapt new methodologies to facilitate their illicit activities. It is now more essential than ever that law enforcement agencies work together to enhance our abilities to address this threat. Currently, HSI uses established investigative techniques that have gradually evolved to keep pace with this change but, HSI often engages its Federal, State, local, and international partners to learn and exchange new and innovative approaches in the cryptocurrency space. HSI leads and participates in numerous task forces and working groups such as, the HSI Cyber Crimes Center, the FBI's National Cyber Investigative Joint Task Force, the U.S. Secret Service's Cyber Fraud Task Force, and the DHS Science and Technology Internet Anonymity Project Working Group.

HSI's extensive international footprint, comprised of more than 80 offices in over 50 countries, equips HSI with a global ability to connect and engage with international partners in this space. HSI special agents assigned to EUROPOL coordinate multi-lateral foreign investigations of darknet markets, cryptocurrencies, and illicit travel connected to terrorism. HSI also sits on multiple committees and engages with international partners to exchange ideas, guide regulatory developments, and exchange investigative information. Given the transnational nature of the crimes HSI investigates, these international partnerships are essential to investigations into cryptocurrency use in illicit and terrorist activities.

Training

HSI has been engaged in a multi-year effort to increase its "cyber-enabled" workforce by training special agents, criminal analysts, and computer forensic analysts to conduct more effective and comprehensive on-line investigations. The HSI headquarters-based financial crimes unit and the HSI Cyber Crimes Center have partnered to provide cryptocurrency and darknet training for HSI special agents, as well as Federal, State, local, and international partners. Since 2017, HSI's subject-matter experts in cryptocurrency have conducted beginner and advanced cryptocurrency training to over 1,000 international law enforcement partners and Government officials world-wide. The training enables U.S. law enforcement agencies to initiate prolonged and combined campaigns of coordinated investigations targeting the criminal organizations that are using cryptocurrencies to launder illicit proceeds derived from various criminal schemes.

Outreach

In 2003, HSI initiated the Cornerstone outreach initiative, a Nation-wide program designed to promote cooperation and collaboration with private-sector partners in order to detect and close vulnerabilities within the financial industry. This mission is accomplished through proactive outreach and collaboration with businesses and industries that manage the very systems terrorists and other criminal organizations seek to exploit. Within the financial sector, HSI's efforts focus on conducting outreach with traditional financial institutions as well as MSBs. With the rapid growth of cryptocurrency, and with it the expansion of private companies involved in cryptocurrency, HSI has expanded Cornerstone to include outreach and training to private industry involved in the cryptocurrency space, who often represent the first line of defense against money laundering and the illicit use of cryptocurrency.

STATISTICS AND INVESTIGATIVE SUCCESSES

While HSI's investigative portfolio is extensive and diverse, financial investigations are at the core of every investigative program area that we investigate. TCOs, terrorist organizations and the myriad of criminal networks have grown increasingly more technical in their approach to obfuscating their criminal acts, while also morphing operations to the perceived anonymity of the darknet. Traditional money-laundering methods remain, yet cryptocurrency can now be used with relative ease to facilitate any type of illicit activity. As such, HSI investigations related to cryptocurrency have risen from one criminal investigation in 2011, to over 604 active criminal investigations in 2021. To date in 2021, HSI has already seized $79,825,606.65 in cryptocurrency. This marked increase signifies growing confidence in cryptocurrency use by bad actors and requires that law enforcement remains technically proficient in performing these complex investigations.

These metrics also reflect an ability of HSI and our partners to engage in a concerted effort to identify and disrupt illicit economies, but to also use that intelligence to disrupt and dismantle the command-and-control structure of TCOs and those that proliferate or support terrorist acts.

To illustrate the above point, HSI led a global cyber operation, along with the Internal Revenue Service (IRS) and Federal Bureau of Investigation (FBI), which resulted in the dismantlement of an on-line infrastructure of Hamas's militant wing, Al Qassam Brigades. Beginning in October 2019, HSI established several undercover personas who executed undercover donation payments, using Bitcoin and undercover electronic communications, with the subjects operating the Hamas cryptocurrency fundraising campaign. The undercover payments were executed in a method that enabled investigators to identify those supporters based in the United States and allowed investigators to further identify money flows. Through additional communications exploitation, HSI was able to identify 64 unique communication channels, which led to the execution of a seizure warrant on a Hamas donor's Bitcoin wallet.

Through additional court-ordered search warrants, HSI identified 64 terrorist-affiliated email addresses, which illuminated the organizational blueprint, as well as covert access of Hamas's on-line recruitment, financing, domain, and network infrastructure, which was spread across the United States, Canada, Russia, Germany, and Saudi Arabia. In July 2020, HSI and IRS special agents executed a total of 24 Federal search and seizure warrants at numerous cryptocurrency exchanges, domain registration providers, VPN service providers, on-line payment providers, DDOS protection providers, and email providers, resulting in numerous account take-overs, server seizures, email account seizures, and domain redirections. Additionally, this cyber operation was executed in cooperation with foreign partners and ultimately resulted in the seizure of terabytes of terrorist-controlled data, the sei-

zure of several million dollars from hundreds of Bitcoin wallets, and the account takeover of a terrorist-administered website that solicits terrorist donations via Bitcoin. This account takeover of website, *www.alqassam.net,* enabled HSI to seize terrorist donations for a 30-day period.

To highlight another investigative example, in 2020, HSI, IRS, and FBI initiated an investigation related to 24 cryptocurrency accounts, all of which were identified as foreign assets or sources of influence for al-Qaeda. This investigation was initiated to investigate the unlawful use of cryptocurrency to support and finance terrorism. As a result of this investigation, HSI subsequently seized 60 virtual currency wallets used in this terrorism financing scheme. The results of this case and others illustrate how law enforcement can effectively disrupt terrorist groups, though the use of HSI's financial and global investigative authorities, technical aptitude, undercover and asset forfeiture authorities and ability to use law enforcement and the private sector as force multipliers in this fight.

GAPS AND SOLUTIONS

While HSI has had success in countering the use of cryptocurrency to facilitate crime, investigative and regulatory challenges still remain. On the investigative front, the pseudo-anonymity offered by cryptocurrencies, combined with enhanced encryption being implemented by some platforms, restricts law enforcement's ability to trace financial transactions between illicit actors in support of a broad range of criminal activities. Cryptocurrency protocols are continuously being refined, and new cryptocurrencies are regularly developed and deployed with ever-growing technological complexity. As a result, law enforcement organizations such as HSI are confronted with the need to continuously update and expand their training and expertise to enable effective investigations. This presents a resource and training challenge, particularly in light of competing priorities within an agency such as HSI with a broad mission set.

Additionally, significant challenges in international regulation remain, including the classification of cryptocurrency, which varies from country to country, and the lack of a common understanding and definition for cryptocurrency and what it is under the law. From HSI's perspective, the implementation of consistent global regulatory oversight would be an important step toward mitigating the illicit use of cryptocurrencies by terrorist and criminal actors. HSI has and will continue to engage with stakeholders across the branches of the U.S. Government to address questions, provide insight, and respond to requests related to cryptocurrency and the digital economy.

CONCLUSION

Thank you again for the opportunity to appear before you today to discuss this important topic and for your continued support of HSI and our investigative mission. HSI remains committed to protecting the physical and digital borders of the United States from TCOs and terrorist networks seeking to exploit and undermine our financial and cyber systems and will continue our efforts at home and abroad to uphold the National security and public safety of the United States.

Ms. SLOTKIN. Thank you for your testimony.

Pursuant to today's order, the subcommittee stands in recess, subject to the call of the Chair.

Mr. Malinowski will be back shortly. I will flag that we have a couple of Members who are on-line. You can't see them, but when they are called for questions, they will come up, and you will be aware of them.

So give us just a few minutes. We will be right back to you.

[Recess.]

Ms. SLOTKIN. The subcommittee will come back to order.

I now recognize Assistant Director Sheridan to summarize his statement for 5 minutes.

Mr. SHERIDAN. Can you hear me, ma'am? I have a red—is that good? Can you hear me? OK.

Ms. SLOTKIN. We can, unless——

Mr. SHERIDAN. OK.

Ms. SLOTKIN [continuing]. The staff can't hear. Let us know. But we can hear you well.

STATEMENT OF JEREMY SHERIDAN, ASSISTANT DIRECTOR, OFFICE OF INVESTIGATIONS, U.S. SECRET SERVICE, DEPARTMENT OF HOMELAND SECURITY

Mr. SHERIDAN. Thank you, ma'am.

Chairwoman Slotkin, Ranking Member Pfluger, and Members of this subcommittee, good morning. Thank you for inviting me here today to testify on how cryptocurrencies, virtual currencies, and other forms of digital money are being used to further advance criminal activity, including acts of terrorism and violent extremism.

My name is Jeremy Sheridan, and I am the assistant director of the Secret Service's Office of Investigations. I lead our more than 160 field offices and direct our global network of Cyber Fraud Task Forces. I work to ensure that the Secret Service is effectively detecting and arresting those engaged in the violations we are authorized to investigate, while also supporting our diverse protective requirements across the world.

For more than 150 years, the Secret Service has conducted investigations to protect the American public, private companies, financial institutions, and critical infrastructure from criminal exploitation. We maintain extensive authorities, expertise, and capabilities to safeguard financial and payment systems from criminal misuse, even as those activities are increasingly transnational and enabled by digital money.

The Secret Service has a distinctive record of success in countering risks related to new technologies. We have successfully investigated and dismantled some of the most notorious virtual money platforms and crypto exchanges and brought to justice some of the most infamous money launderers and cyber criminals in U.S. history.

Today, we remain committed to keeping pace with innovation and the evolving strategies and tactics criminals are using to exploit new financial instruments.

Our perspective on these matters is based on our unique role. We are not a financial regulator or a member of the intelligence community. We are a law enforcement agency focused on accomplishing our integrated mission of protecting designated persons, places, and events and investigating crimes that undermine the integrity of financial and payment systems. This unified mission necessitates that we understand how digital money may present risk to the Nation's financial system as well as to our many protectees.

Consequently, today, I will aim to address the broad criminal risks of digital money as well as the work of the Secret Service and our partners to mitigate those risks. I believe the measures to investigate and address these risks apply equally to violent extremism and financially motivated crime as they do to other forms of criminality.

I wish to stress that, while digital money is not inherently criminal, it can be abused and is currently being abused for a wide variety of criminal purposes, from money laundering and ransomware to illicit financing of terrorism and violent extremism.

Over the past decade, law enforcement has made great strides in the fight against the illicit use of digital money, but we anticipate that the on-going growth and criminality will continue over the coming years. Organized crime groups, terrorists, and other bad actors will continue to view digital money as an effective means to transfer value globally and as a means of evading the anti-money-laundering controls that are well-established within the traditional financial system.

As the cryptocurrency industry improves their compliance with anti-money-laundering obligations, the Secret Service is focused on staying one step ahead of our adversaries. By building the investigative capabilities and purview to meet the evolving threats, we can continue to detect and arrest those who engage in criminality using digital money.

But we must not be complacent. Keeping pace with criminals requires a continuous investment in technology, training, and, most importantly, people. The investigation of cyber crime and illicit finance is complex, demanding work. We need a steady stream of bright, diligent professionals equipped with the latest technology, training, and expertise if we hope to continue to be successful in the future, as we have in the past.

Allow me to reiterate what many of my predecessors have emphasized. Those that seek to further their illicit activities through the use of digital currencies or the internet, more broadly, should have no illusions that they are beyond the reach of law. Even those digital assets and services that claim to be anonymous can be tracked and interdicted.

As the investigative work of the Secret Service and our partners has demonstrated over the decades, we in law enforcement, whether it be the Secret Service, the FBI, HSI, IRS CI, or any of the other investigative agencies of the U.S. Government, are relentless in enforcing the law. We will not stop until those who seek to harm the United States and its citizens are arrested, convicted, and punished.

Chairwoman Slotkin, Ranking Member Pfluger, and Members of this subcommittee, thank you again for the opportunity to appear before you today and for your continued support of the U.S. Secret Service. I look forward to working closely with this committee and with other Members of Congress on our shared priorities and welcome your questions.

[The prepared statement of Mr. Sheridan follows:]

PREPARED STATEMENT OF JEREMY SHERIDAN

JULY 22, 2021

INTRODUCTION

Good morning Chairwoman Slotkin, Ranking Member Pfluger, and Members of this subcommittee: Thank you for inviting me to testify on how criminals use digital money,[1] including cryptocurrencies, to further illicit activity, such as terrorism and

[1] The term "digital money" is used to refer to a representation of value that is stored on and transferred through computer systems and that is used similar to money, regardless of legal tender status. The term "digital money" is inclusive of, but is not limited to, cryptocurrency assets like Bitcoin, Ether, Tether, and others. Consistent with FinCEN guidance (FIN–2013–G001), the Secret Service uses the term "virtual currency" to refer to mediums of exchange that operate like currency, but do not have legal tender status.

unlawful acts of violent extremism. My name is Jeremy Sheridan and I am the assistant director of the Office of Investigations. In this role, I lead more than 160 Secret Service field offices and direct our network of Cyber Fraud Task Forces (CFTFs) in their investigations of sophisticated computer and financial crimes. I ensure our global network of field offices and task forces effectively detect and arrest those that are engaging in the criminal violations we are authorized to investigate,[2] while fully supporting our diverse protective requirements across the world.

Today, I will provide you with an overview of the risks associated with digital money, as viewed from the perspective of the United States Secret Service (Secret Service), and to highlight the various actions we are taking to address those risks. As part of my testimony, I will also seek to highlight some key challenges that we see on the horizon.

For more than 150 years, the Secret Service has conducted investigations to protect the American public, private companies, financial institutions, and critical infrastructure from criminal exploitation. We maintain extensive authorities, expertise, and capabilities to effectively safeguard financial and payment systems from criminal misuse, even as those illicit activities are increasingly transnational in nature and enabled by the internet.[3]

The Secret Service has a distinctive record of success in countering risks related to emerging financial and payment technologies. This includes countering fraud in electronic transfers of funds in the early 1980's, countering criminal schemes related to payment cards in the 1990's, and investigations related to cryptocurrencies and digital money platforms over the past decade and half. Today, we remain committed to keeping pace with technological innovation and the evolving strategies and tactics criminals are using to exploit these new financial instruments.

Through our decades of criminal investigations, the Secret Service has developed a deep understanding of the risks, challenges, and potential investigative benefits of digital money, as well as the effectiveness of various potential law enforcement and regulatory responses. Our perspective on these matters is based on our unique role. We are not a financial regulator or a member of the intelligence community. We are a law enforcement agency focused on accomplishing our dual responsibilities of protecting designated persons, places, and events and investigating crimes that undermine the integrity of financial and payment systems. These unified mission sets necessitate that we understand how digital money may present risks our Nation's financial system, such as through money laundering, fraud, theft, and extortion by cyber criminals (including through ransomware), in addition to the ways in which they present risks to our many protectees.

Consequently, my testimony today will address the broad risks of how criminals can use digital money. In the interest of protecting on-going investigative activities and other law enforcement sensitive information, I will avoid detailed discussion of specific recent events or law enforcement techniques. I believe this committee's work can be well-informed by a discussion of the broad range of illicit activity that is enabled by digital money. The measures to investigate and address these risks, I believe, apply equally to terrorism, violent extremism, and financially-motivated crime, as they do to other forms of criminality.

SECRET SERVICE INVESTIGATIONS OF DIGITAL MONEY

The commercialization of the internet in the 1990's brought with it a new push to develop payment systems that could function effectively within a digital economy. While the U.S. market predominately adopted payment cards as the solution, there have been numerous attempts to develop new digital payment systems that could operate with greater independence from, and with a similar degree of trust to, the traditional financial system, and all at a potentially lower cost. In 2009, Bitcoin sought to achieve these goals through a novel approach of using public-key cryptography and on-going decentralized computation to form a blockchain, a technical architecture which forms the basis of most forms of digital money today.[4]

Since that time, the popularity of Bitcoin has inspired an exponential growth in digital assets globally, from cryptocurrencies to stable coins to non-fungible tokens (NFTs). As of July 2021, there are more than 5,000 blockchains in operation on the internet, with over 300 million users world-wide and total market capitalization of

---

[2] See 18 U.S.C. §§ 1028–1030, and 3056(b).

[3] For more information on the Secret Service's investigative mission see: *https://www.secretservice.gov/investigation*.

[4] Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008). Last accessed on July 6, 2021. Available at: *https://bitcoin.org/bitcoin.pdf*.

approximately $1.43 trillion.[5] Even central banks are exploring these technologies as a means of encouraging more transparent and seamless financial exchanges. Several are already in circulation.[6] While much of this effort is in support of legitimate economic activity, the rapid expansion of cryptocurrencies, as well as other digital stores of value, presents a significant challenge to law enforcement, and a growing area of risk to the United States and our foreign partners.

The Secret Service has been at the forefront of combatting these crimes from their earliest iterations, and we continue this work today. We have successfully investigated and dismantled two centralized virtual currency providers that supported extensive criminal activity: e–Gold Ltd. (in 2007)[7] and Liberty Reserve (in 2013).[8] Working with our partners, we investigated and ultimately shut down a number of other virtual currency exchangers,[9] including Western Express,[10] which was prosecuted by the Manhattan District Attorney's Office, and, in 2017, the cryptocurrency exchange BTC–e.[11] Through a partnership with the Internal Revenue Service's Criminal Investigation Division (IRS–CI) and other foreign and domestic law enforcement agencies, we successfully shuttered BTC–e, after it was accused to have failed to implement a program to prevent illicit financing.[12]

More recently, in collaboration with our Federal and international partners, we successfully investigated a highly sophisticated, Russia-based criminal scheme to defraud multiple cryptocurrency exchangers and their customers.[13] This effort led to the seizure of millions of dollars' worth of virtual assets. The criminals indicted in this scheme are alleged to have employed a variety of advanced methods in support of their fraud, including using fictitious or stolen identities to create accounts; circumventing exchanges' internal controls; swapping and mixing different types of virtual currency; moving virtual currency through multiple intermediary addresses; and a market manipulation scheme in which inexpensive virtual currency was purchased at a fast rate to increase demand and price, then quickly sold for a higher price to make a quick profit.

And just this year, our work investigating illicit uses of cryptocurrency supported indictments and arrests associated with a vast money-laundering operation that provided criminal services to not only some of the world's most dangerous cyber

---

[5] "Cryptocurrency Prices by Market Cap," Last accessed on July 6, 2021. Available at: *https://www.coingecko.com/en.*

[6] Among others, the Central Bank of Sweden proposed an "e-krona" in November 2016, and started testing an e-krona proof of concept in 2020; in November 2017, the Central Bank of Uruguay announced to begin a test to issue digital Uruguayan pesos; and on October 20, 2020, the Central Bank of the Bahamas introduced the "Sand Dollar" as a digital legal currency equivalent to the traditional Bahamian dollar. See Deloitte, "Are Central Bank Digital Currencies (CBDCs) the money of tomorrow?" Last accessed on July 11, 2021. Available at *https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu-are-central-bank-digital-currencies.pdf.*

[7] See U.S. Department of Justice: "Over $56.6 Million Forfeited In E-Gold Accounts Involved In Criminal Offenses," *https://www.justice.gov/usao-md/pr/over-566-million-forfeited-e-gold-accounts-involved-criminal-offenses;* Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting, *https://www.justice.gov/archive/opa/pr/2007/April/07_crm_301.html.*

[8] See U.S. Department of Justice press releases: "Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million through His Digital Currency Business," *https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital;* "Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One Of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A $6 Billion Money Laundering Scheme," *https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-liberty-reserve-one-world-s-largest.*

[9] Exchangers are businesses that allow for the trade of digital currencies for other assets, such as conventional fiat money, such as U.S. dollars, or other digital currencies.

[10] See Manhattan District Attorney, "DA Vance Testimony on Digital Currency before the Department of Financial Services," *https://www.manhattanda.org/da-vance-testimony-on-digital-currency-before-the-department-of-financial-services/.*

[11] See, "Russian National and Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox," *https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged.*

[12] See, "FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales" *https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware.*

[13] See, "Russian Nationals Indicted for Conspiracy to Defraud Multiple Cryptocurrency Exchanges and Their Customers," *https://www.justice.gov/usao-ndca/pr/russian-nationals-indicted-conspiracy-defraud-multiple-cryptocurrency-exchanges-*; and "Treasury Sanctions Russian Cyber Actors for Virtual Currency Theft," *https://home.treasury.gov/news/press-releases/sm1123.*

criminals but also North Korean military-affiliated actors.[14] This North Korean group is accused of creating and deploying multiple malicious cryptocurrency applications, of developing and fraudulently marketing a fictitious blockchain platform, and ultimately stealing more than $1.3 billion from victims in the United States and overseas.

During the course of our criminal investigations, the Secret Service maintains close and continuous partnerships with a wide range of domestic and international law enforcement agencies. We regularly coordinate our work with the Department of Justice, Federal Bureau of Investigation (FBI), Homeland Security Investigations (HSI), IRS–CI and others, and, where appropriate, conduct joint investigations and information sharing with foreign counterparts. Through our Cyber Fraud Task Forces and through domestic and international task forces, like the National Cyber Investigative Joint Task Force (NCIJTF) and the Joint Cybercrime Action Taskforce (J–CAT) in Europe, we work to ensure effective deconfliction and intelligence sharing between and among our law enforcement partners.

COUNTERING RISKS INVOLVING DIGITAL MONEY

Criminals can abuse digital money for a wide variety of purposes, including in support of terrorist or violent extremist activities. The types of criminality are diverse, and include such schemes as crypto-jacking,[15] thefts of private keys,[16] the purchase of illicit goods or services on the dark web, attacks on block chain networks,[17] money-laundering, sanctions evasion, illicit financing, and as the extortion payment method of choice in modern ransomware, among other potential crimes.[18]

The blockchain analysis tracking firm Chainalysis, has identified approximately $21.4 billion worth of likely illicit cryptocurrency transfers in 2020.[19] However, we believe that this is likely a significant underestimate of the total value of illicit cryptocurrency transfers. Certain blockchain implementations on specific currencies can provide information for insightful analysis on its own, but a full accounting of the motives and identities of criminal actors using these tools can only be achieved through the work of trained criminal investigators, armed with subpoena powers and court-sanctioned legal process to undercover the true scale of the problem.

A 2019 study[20] on terrorist use of digital currencies by the RAND Corporation, supported Secret Service's Office of Investigations finding that a specific digital currency can be viewed as more or less appealing to bad actors based upon six criteria: A currency's level of anonymity, its usability, its security, its acceptance in the marketplace, its reliability, and its overall volume. RAND's research shows that, "should a single cryptocurrency emerge that provides wide-spread adoption, better anonymity, improved security, and that is subject to lax or inconsistent regulation, then the potential utility of this cryptocurrency, as well as the potential for its use by terrorist [or criminal] organizations, would increase." It is thus essential that the U.S. Government keep pace with changes in the market and align investigative resources and regulatory oversight to shifts in the tactics of terrorists, criminals, and other bad actors.

Law enforcement has made tremendous strides in the fight against illicit use of digital money, but we anticipate that the on-going growth in criminality will continue in the coming years. Organized crime groups, terrorists, violent extremists,

---

[14] See, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," *https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and*.

[15] Crypto-jacking is the use of malware or compromised websites to use, without authorization, computing power of others for cryptocurrency mining. Mining is the computational process that verifies and maintains a blockchain, and is typically incentivized by a blockchain protocol rewarding cryptocurrency to miners.

[16] Control of assets on a blockchain is maintained through exclusive control and access to the associated private cryptographic key; however, there have been numerous instances of cryptocurrency heists, involving major exchanges, wallets, and individual users resulting from the theft and illicit use of private cryptographic keys.

[17] We have observed a few instances of attacks on blockchain systems themselves, either to impair their operation, as part of a broader scheme, or as part of a "51 percent attack" to defraud other users of the cryptocurrency. Such activities typically involve violations of 18 U.S.C. § 1030 and can also include other criminal offenses.

[18] Ransomware, which impairs the operation of a computer as part of an extortion demand, has substantially grown in threat, corresponding with adopting cryptocurrencies as the means of paying extortion demands.

[19] "Crypto Crime Report 2021," Chainalysis, available at: *https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf*.

[20] See, "Terrorist Use of Cryptocurrencies Technical and Organizational Barriers and Future Threats," The RAND Corporation, 2019, available at *https://www.rand.org/pubs/research_reports/RR3026.html*.

and other bad actors will continue to view cryptocurrencies as an effective means to transfer substantial values globally, without encountering the anti-money laundering controls common in the traditional financial system. As the cryptocurrency industry improves their compliance with anti-money laundering (AML) obligations, I am focused on keeping the Secret Service one step ahead of our adversaries. By developing the investigative capabilities and purview to meet the evolving threat landscape, we can continue to detect and arrest those engaged in crime, including those engaged in terrorism and violent extremism.

CHALLENGES FOR FURTHER CONSIDERATION

Cryptocurrencies remain attractive to bad actors for the various reasons provided above, but it also has its limitations and criminal drawbacks. For cryptocurrencies or other digital assets to be utilized within the mainstream economy—namely, to exchange them for most goods or services—they usually must be converted into government-backed fiat currency, such as the U.S. dollar, European euro, or Chinese yuan. This conversion typically occurs through "exchanges," money services businesses which allow for the purchase and sale of digital assets with fiat currency. Exchanges, both as on-ramps and off-ramps to the cryptocurrency economy, have been a particularly effective data source and control point for governments to focus their efforts; however, as the variety of digital assets increases, further attention is needed to address the risks of technologies and services that obscure digital transactions from law enforcement and regulatory oversight.

The United States and the broader international community have spent decades developing, implementing, and strengthening a global anti-money laundering (AML), Know-Your-Customer (KYC), and countering the financing of terrorism (CFT) regime. Financial institutions doing business in the United States must follow a host of statutory and regulatory obligations, including those related to the Bank Secrecy Act of 1970, the Annunzio-Wylie Anti-Money Laundering Act of 1992, and the Money Laundering Suppression Act of 1994, in addition to other associated laws and Federal regulations. These laws require covered entities to be registered, establish compliance programs, due diligence systems and monitoring programs, transmit suspicious activity reports, and develop risk-based anti-money-laundering programs. Failing to comply with these requirements or conducting or facilitating transactions designed to avoid reporting requirements or conceal or promote specified unlawful activities may constitute criminal violations of Title 31 of the U.S. Code or sections 1956, 1957, or 1960 of Title 18, in addition to other provisions of U.S. law.

Criminals and terrorist groups persistently seek to avoid U.S. and foreign AML and KYC requirements by utilizing exchanges that do not adhere to these laws or reporting requirements. Criminals are also increasingly exploiting over-the-counter (OTC) brokers, which facilitate transactions conducted directly between two parties through bilateral contracts. Unlicensed OTC brokers with weak AML/CFT programs are increasingly being used by criminals and other bad actors for money laundering and other financial crimes. Compared to institutional exchanges, OTC brokers provide a more decentralized approach, which makes them attractive for those intent on engaging in money-laundering activity. In both cases, with exchanges or OTCs, criminals look to utilize those providers hosted in foreign jurisdictions with lax AML requirements or weak enforcement.

Accordingly, it is vital to U.S. National security that AML/KYC laws achieve their intended effects, regardless of the bad actors' motivations for exploiting them. The enactment of the Anti-Money Laundering Act of 2020 (AML 2020) was an important step in this direction. Timely and effective implementation of the rules directed by this law, and effective enforcement of violations, will likely have a substantial impact on the illicit market.

We are closely monitoring and participating in the implementation of the AML Act of 2020, both to track potential emerging risks and to identify where further action may be helpful. For example, enhanced data reporting, collection, retention requirements, and accessibility requirements may strengthen criminal investigations and effective oversight. We also foresee significant money laundering risks, which may require further action, related to anonymity-enhanced cryptocurrencies, services intended to obscure transactions on blockchains (i.e., cryptocurrency tumblers or mixers), and cryptocurrency mining pools.

That said, the United States should be cautious about acting unilaterally, as this can simply lead to the "offshoring" of cryptocurrencies and associated services to foreign jurisdictions. We believe that the most effective interventions are those that are conducted in coordination with other major economic powers. Our foreign partners perform critical roles in in assisting U.S. law enforcement with conducting investigations, making arrests, seizing criminal assets, and establishing effective AML

regulations to counter transnational criminal activity that harms Americans. As we take steps domestically, we continue to work to ensure that foreign partners are willing and capable to assist us in investigations. To that end, the Secret Service continues to partner closely with Departments of State, Justice, and the Treasury to develop these essential foreign partnerships and work collaboratively on multinational criminal investigations and training programs.

Further, we acknowledge that some exchangers or brokers may actively obfuscate their ownership and location in an effort to evade detection and oversight. To address this challenge, additional consideration is warranted to improve cooperation between U.S. Government authorities and foreign and domestic providers of electronic communications services and remote computing services. This will facilitate expeditiously identifying users engaged in certain illicit activities, such as those involving digital money laundering, transnational cyber crime, or terrorist financing. Last year, the Cyberspace Solarium Commission made important recommendations toward achieving such improved cooperation.[21]

Strong overseas partnerships are also key to effective regulation and oversight. Fostering these partnerships requires continual investment in government-to-government law enforcement and regulatory relationships to develop shared understanding of risks, and to ensure an effective international anti-money laundering regulatory and enforcement programs. Toward this end, we welcome efforts to improve global controls related to digital assets, through our international partners, and other global financial and banking associations.

Finally, investigating crimes involving digital money, and the transnational organized criminal and terrorist groups that exploit it, requires highly-skilled criminal investigators. Hiring, developing, retaining, and equipping our investigative workforce, as well as partnering with and training our domestic and foreign law enforcement and other partners to develop their investigative capabilities, are all critical priorities for ensuring that the United States is well-prepared to address emerging risks both today and into the future.

This can be achieved by strengthening and growing law enforcement training and capacity-building programs that equip Federal law enforcement, and our partners, with the technical skills and tools necessary pursue the most sophisticated transnational criminals. Programs such as the Secret Service's National Computer Forensics Institute (NCFI), which yearly trains over 3,000 U.S. State and local law enforcement officials in computer investigations techniques, and the Department of State's International Law Enforcement Academies (ILEA), which provide instruction to foreign law enforcement partners on approaches to combatting cyber crime and illicit finance, are prime examples of initiatives that enhance these requisite capabilities.

CONCLUSION

Digital money is clearly of great interest to governments, businesses, and U.S. citizens, as demonstrated by the substantial research conducted and investments places into these assets. The Secret Service is focused on doing our part to address the challenges posed by the increasing use of digital money in furtherance of illicit activity, from ransomware, to money laundering, to the financing of violent extremists and terrorists. But we and our law enforcement partners, both domestic and foreign, must and can do more. We must dramatically expand our efforts, and continue to adapt our investigative tools and techniques, if we hope to stem the tide.

Chairwoman Slotkin, Ranking Member Pfluger, and Members of this subcommittee, I will conclude by reiterating what many of my predecessors have emphasized here before in this body: Those that seek to further their illicit activities through use of digital currencies, or the internet more broadly, should have no illusions that they are beyond the reach of the law. Even those assets and services that purport to be "anonymous" can be tracked and interdicted. As the investigative work of the Secret Service and our law enforcement partners has over the years demonstrated: We are relentless in enforcing the law and will not stop until those who seek to harm the United States and its citizens are arrested, convicted, and punished to the fullest extent of the law.

Thank you again for the opportunity to appear before you today, and your continued support for the mission of the U.S. Secret Service. I look forward to working closely with this committee, and with other Members of Congress, on our shared priorities. I look forward to answering your questions.

---

[21] See, The Cyberspace Solarium Commission Report, available at, *https://www.solarium.gov/report*.

Ms. SLOTKIN. I thank all the witnesses for their testimony.

I will remind the subcommittee that we each have 5 minutes to question the panel. Since we haven't been in the room for a while, the clock is under the screens. That is 5 minutes total, so I will give you a gentle tap of the gavel when you have hit your 5-minute mark, if you are going strong.

I will now recognize myself for questions.

So, Ms. Dobitsch, can you help us just contextualize the threat? You know, sort-of, we know that there is, you know, a number—there is a bunch of terrorist organizations, there is a bunch of domestic extremist organizations that threaten Americans in different ways. How significant is the use of cryptocurrency versus other types of currencies, versus traditional types of currencies? I know it is hard to put an exact percentage on it, but give us a sense of the scale, if you would.

Ms. DOBITSCH. Thank you, Chairwoman.

In terms of the scale, I think from a terrorist perspective we are really in the nascent stages, particularly as we look at foreign terrorist groups overseas. They remain reliant on those traditional sources of funding. But we are seeing increasing use of cryptocurrency, particularly regarding soliciting donations and fundraising. So early on in the stages.

I think from a criminal perspective it is becoming more mainstream. Obviously, we are seeing more activity from transnational criminal organizations, obviously from cyber criminals, and, in certain instances, nation-states that are using it more frequently than they are those traditional sources.

I think, as the technology becomes more accessible and easier for the user, it is going to be more common among terrorist groups. Again, it is largely limited. We have seen several cases. But, again, I think the concern for us is that as the technology advances and becomes more user-friendly that we are going to see more activity.

Ms. SLOTKIN. Mr. Eisert, can you help us understand the use of sites that Americans are really used to, like GoFundMe, you know, Amazon, to raise money for charity? You know, most Americans have seen someone at least advertise those kinds of campaigns. Can you talk to us about what, if any, abuse you see of those sites?

Mr. EISERT. Sure. Luckily for us, a lot of those mainstream payment systems, like PayPal and GoFundMe, they have due-diligence systems in place and checks and balances. So a lot of the social media sites and those mainline payment systems have identified criminal activity and have pushed them off the networks.

But that is why—that is one of the reasons why we are starting to see an increase into these alternate forms of payment systems, like virtual currency.

Ms. SLOTKIN. Then I think for both Mr. Eisert and Mr. Sheridan, just tell us about—you know, I have assumed that from a law enforcement perspective it is just harder to go after, you know, groups that are using cryptocurrency as opposed to traditional currencies.

What are the tools or legal authorities that either you don't have, that you want to have, that would make your life easier? What are the roadblocks that are holding you back?

Mr. SHERIDAN. That is a really important question, ma'am. Thank you.

So, in regards to your first question about tools, we in the Secret Service rely on our Cyber Fraud Task Forces that are stationed globally and partner with all of Government in order to combat this threat. What we need in order to expand is to increase our presence in the international setting. As was mentioned earlier, this is an international/transnational crime situation that we are facing, and we need to increase our presence there.

We need to get better at our processes in order to ensure that we are aggregating data appropriately and conducting the necessary data-link analysis for attribution.

We need to continue to modernize. We greatly appreciate Congress's help in the Cyber Fraud Task Force modernization that they have assisted us with, but we need to continue to grow in those areas.

As it relates to authorities, similarly, ma'am, there are areas for growth as it relates to our investigative authorities related to money laundering, structured payments, and unlicensed money transmitters that would make us stronger in this fight.

Ms. SLOTKIN. OK. Well, I am sure we would love to hear more about some of the details.

Then to Ms. Dobitsch again: You know, we know that intelligence is an important part of understanding these organizations and how they finance themselves. Talk to us about, like, what does the interagency structure look like in the Government? Who is working on this? Who do you talk to every day? Is there actually coordination between different actors?

Ms. DOBITSCH. Yes, ma'am, it is certainly an interagency problem.

I think the difficulty really is thinking about that end-user. So we are seeing the activity occurring, but oftentimes we have significant information and intelligence gaps about where that money is going and how it is ultimately used.

I&A certainly serves as that bridge between law enforcement and the intelligence community. In addition to that, it really takes not just an individual or an intelligence officer that kind-of understands the intent and capabilities of the actor but also has that deep understanding and knowledge of the technology itself.

If you look at a group like ISIS, in terms of their use of drones, really, since 2014, they rapidly expanded their capability to leverage drones, first for reconnaissance and then for actual attacks on the battlefield overseas.

So it really takes a whole-of-Government effort and connecting that law enforcement information with the intelligence to get the fullest picture of the threat.

Ms. SLOTKIN. Great.

I now recognize Ranking Member Mr. Pfluger for questions.

Mr. PFLUGER. Thank you, Chairwoman.

I am so glad you brought up the use of drones. I think the key here is that they are using an innovative approach, and the nature of warfare is constantly changing, and we have to stay one step ahead.

So I appreciate your testimonies so far and wanted to get right into some questions with Mr. Eisert.

I understand that cryptocurrency has attracted bad actors because of the pseudo-anonymity or anonymity, in some cases. I want to focus now on the cartels. Have you seen cartels using cryptocurrencies in order to hide illicit proceeds from transnational criminal activity?

Mr. EISERT. Yes. Thank you for that question.

Yes, we do have recent investigations where we do see cartels conducting business with money brokers, professional money launderers. Throughout our investigations, we target these professional money launderers and insert our undercover activities with them.

Specific to the cartels, we have found ourselves in the middle of investigations picking up cartel-level street proceeds and converting them to cryptocurrency through peer-to-peer platforms.

Mr. PFLUGER. How easy is that, for them to translate that into—to either leverage for what they want to get out of it for the use of, you know—into and out of the United States?

Mr. EISERT. Oh, once it is in the virtual currency format, it could be moved around the world in a matter of minutes, 100 times over around the world.

The biggest chokepoints and where we have our most success is when the on-ramping or the off-ramping of the virtual currency, so, for instance, getting it into the virtual currency realm. That is where we have our success in our undercover platforms and through our traditional money-laundering investigations.

A few years back, many of the mainline exchanges were regulated as money service businesses and needed know-your-customer regulations, and that has pushed a lot of the illicit activity to unregulated peer-to-peer atmosphere. That is where we primarily target the cartel and their work.

Mr. PFLUGER. Thank you very much for that.

For Mr. Sheridan, how does the Secret Service's approach differ from other agencies, other law enforcement colleagues? Kind-of, what makes you and the Secret Service unique in this regard?

Mr. SHERIDAN. Thank you for that question, sir.

So all law enforcement entities bring their own unique set of capabilities to this fight. We in the Secret Service are a smaller organization. That makes us more agile for information sharing and case coordination within our own agency.

That small size also requires us to rely on partnerships. Partnerships are the lifeblood of the Secret Service, not only in our protective mission but investigatively as well. So we develop very strong partnerships across all of Government and with our international law enforcement partners.

We also have a unique methodology, in that we have been doing this for 150 years. We have, over the past several decades, created a database of information related to these cyber actors, many of whom have graduated up to these most complex cyber-enabled fraud schemes that we are seeing today. We are able to follow that digital link to when they were just starting out and had a more public—and weren't as concerned with their on-line presence as being so noticeable.

Then I think our perspective. Our perspective is based on our focused statutory authority, which is to protect the Nation's financial payment systems and financial infrastructure. That allows us to be specialists, as opposed to generalists, and create, really, subject-matter experts within our organization to conduct these investigations.

Mr. PFLUGER. Thank you for that.

Let me just talk about the whole-of-Government approach. I appreciate your comments on that, Ms. Dobitsch. For me, representing a university that is a cyber center of excellence, talk to me about that whole-of-Government approach, the private-public partnerships that you all, I think, have mentioned, and how we can leverage a university like Angelo State University, who focuses on this—and, by the way, a minority-serving institution, a Hispanic-serving institution, doing wonderful things. Talk to me about how we can incorporate students and their learning and what they should be focusing on so that they can enter your organizations and combat this.

Ms. DOBITSCH. Yes, sir. Absolutely. As I stated earlier, having a sophisticated understanding of the technology itself is the first step, and that often comes from private business and academia. Understanding the trends that exist in cryptocurrency and other digital currencies is really that first step.

Then, also, learning more about the vulnerabilities of each of those types of currencies. From the Classified intelligence perspective, we have the intent and capabilities of those actors, but we can only understand really what the threat is if we know well what the technology is able to do and what security mechanisms are in place to prevent the malicious use of that currency or other technology.

So it really is a partnership. It is not just intelligence. That is why we say "information and intelligence." It is that law enforcement data, it is the private academia, and, really, all sources of information, because this is a global trend, it is a global technology, and all types of actors are really seeking to exploit the technology for their own benefit.

Mr. PFLUGER. Well, thank you for that.

We need to know the resources that you need. We need to know the things that you identify, what we are talking about here. If there is a more comprehensive list, we need to know that.

We have seen it in the ransomware attacks recently. You have mentioned it in many of the examples you have given us. But that is the purpose of this hearing and the purpose of our committee, is to give you those resources, if we can, to make sure that we can combat that.

With that, Madam Chair, I yield back.

Ms. SLOTKIN. The Chair will now recognize other Members for questions they may wish to ask the witnesses. In accordance with the guidelines laid out by the Chairman and Ranking Member in the February 3 colloquy, I will recognize Members in order of seniority, alternating between Majority and Minority.

Members participating virtually are also reminded to unmute themselves when recognized for questioning.

The Chair recognizes for 5 minutes the gentleman from New Jersey, Mr. Malinowski.

Mr. MALINOWSKI. Thank you. Thank you, Madam Chair.

So, as all of you have testified, cryptocurrencies are being used right now for all kinds of very nefarious purposes—to purchase illicit goods, drugs, guns; to provide material support to terrorist organizations; to enable the ransom payments that are fueling arguably the biggest threat, one of the biggest threats, that Americans are facing in their daily lives today.

Mr. Eisert, I think you said in your testimony that they give bad actors the ability to engage in money laundering with minimal effort. That is pretty bad.

Just so everybody is clear, maybe say a little bit more about that. What is it about cryptocurrency that enables somebody to engage in money laundering with minimal effort?

Mr. EISERT. Absolutely. Thank you for that question.

The cryptocurrency problem set transcends borders, transcends industries. What I mean by that is, as I discussed earlier, once you can get your money into the crypto world through a regulated exchanger or an unregulated exchanger, it is a push of the button.

I could tell you about the old days of law enforcement of following money launderers from bank to bank, and good luck if they could hit 20 in a day. Now you can sit on your couch and move it 100 times over. There is one documented case where money was moved over 21,000 times before it came out.

Mr. MALINOWSKI. Yes.

Mr. EISERT. It is that simple. So, once it is in the system, it is moving.

Tracing it within the system, it is challenging but not unbelievable. Identifying who is attached to that transaction is the challenge.

Mr. MALINOWSKI. Well, here is what troubles me. Chairwoman Slotkin, in her opening statement, said that there is nothing inherently wrong with digital currency. I could be convinced of that, but I am not convinced of that, because I am trying to see the other side.

With, for example, drone technology, we know drones can be used for deadly, nefarious purposes, including some we have not yet seen that we all fear. Yet all of us can list dozens of positive uses of drone technology for consumers, for companies.

Maybe you are not the right people to ask this question to, but can you think of any socially beneficial uses of cryptocurrency beyond providing some people with something to speculate in and make money off of?

Mr. EISERT. Well, coming from the law enforcement side, we are always looking at the illicit side. So I can only tell you what my beliefs are and what is out there on the open web. I believe a lot of that focus goes into the underbanked. It gives an opportunity for the underbanked areas and countries to engage in world-wide transactions.

Mr. MALINOWSKI. Well, I don't know. I mean, I hear things like, well, it provides privacy. That didn't stop us from—and I am deeply committed to privacy. It did not stop us from banning the use of anonymous shell companies for very similar reasons, right? Because they are used to cover up illicit activity.

I hear the phrase that it enables the democratization of currency. Every time someone says we are democratizing something, it kind-of ends the conversation. That is sort-of good. I don't really understand what that means in this context. I think it is an abstraction, whereas ransomware attacks are not an abstraction. They are hurting people every single day.

So I am not sure if I see it. I think we do need to expand this conversation to ask that fundamental question, whether the challenges that you are facing, that we are asking you to deal with, in protecting us against all of these social ills, are challenges that are necessary, inescapable, and inevitable. I think we have to ask, what is the good, what is the positive social value of this phenomenon that is also creating all of this harm?

You know, I think when you look at the history of how we built modern economies in the United States and around the world, we started 300 or 400 years ago with multiple currencies that were unregulated and not controlled by governments, and in every modern economy we built what we have today when Government decided, no, we are going to have one currency that is issued and regulated by Government.

I think I could ask you—we don't have time—how we can better regulate cryptocurrency, but I think if we regulated it, it wouldn't be crypto anymore, and so what would be the point? So I come back to the question, should this be allowed?

Thank you. I yield back.

Ms. SLOTKIN. The Chair recognizes for 5 minutes the gentleman from Mississippi, Mr. Guest.

Mr. GUEST. Thank you, Madam Chairman.

Director Sheridan, you say in your written testimony that for cryptocurrency and other digital assets to be utilized within the mainstream economy, they usually must be converted into Government-backed currencies, such as the U.S. dollar and the euro.

You said that exchanges serve both as on-ramps and off-ramps to the cryptocurrency economy. You talk about the growth of unlicensed over-the-counter brokers and the importance of anti-money-laundering and know-your-customers laws.

Could you expand on that very briefly?

Mr. SHERIDAN. Yes, sir. Thank you for that question.

What my written testimony was meant to encapsulate is the ecosystem of what we refer to as digital money. We see in a lot of these conversations that the terms related to the different platforms are used interchangeably: Virtual currency, digital currency, cryptocurrency. We in the Secret Service use the term "digital money," because that encapsulates all forms, to include cryptocurrency and the most commonly referred to coins, such as Bitcoin, Ethereum, Tether, and so forth.

The true definition really comes down to the technology used to create it, the regulations that apply, whether or not it is legal tender. But, for us, it comes down to how it is used.

So the written testimony is meant to describe in more detail how it is used, as my colleague has identified, to on-ramp from legal tender to digital money, how it is used laterally for legal and illicit means, and how it is off-ramped, converted away from a digital platform to legal tender.

The exchangers that were referenced are certainly integral to that. These are the ways in which we in law enforcement find are primary means to engage for identification and further information related to the digital money that is used.

Mr. GUEST. Switching gears very quickly, back in April, there was an announcement that the Secret Service was going to partner with the Mississippi attorney general's office, various other local law enforcement agencies, in establishing a Mississippi Cyber Fraud Task Force.

My question is two-fold. One, can you talk a little bit about the importance of these task forces, how that serves as a force multiplier to what you are trying to do in the Secret Service?

Then the other thing I want to follow up on is, it is my understanding that all of these agents will be trained at the National Computer Forensics Institute, which is located at Hoover, Alabama. I am very familiar with that institute. But can you talk a little bit about the mission of that institute and the important role that that organization serves?

Mr. SHERIDAN. Yes, sir. The Cyber Fraud Tasks Forces are our global network of investigative task forces staffed by not only our special agent personnel but our professional work force of subject-matter experts from our Investigative Services Division, our network intrusion forensics analysts. These are our touchpoints to the local communities, to your constituents, that bring the information back to our Global Investigative Operations Center to make the whole Secret Service approach to our investigations.

As you said, sir, a lot of what we do on that local level is through the National Computer Forensics Institute. As you are aware, that is the only Federal facility to train and equip State, local, territorial, Tribal officers, judges, and prosecutors. Those officers and law enforcement entities are really the first responders. They are the front line, they are the surge capacity in this fight against the complex cyber-enabled fraud.

We are very grateful for the support of Congress for the growth of that facility. We have trained over 16,000 of those law enforcement officials. But, as you are aware, that facility's authorization is due to sunset in 2022, and we would greatly appreciate the support to continue its authorization, not only domestically but to expand that same training to our foreign partners to take this fight globally, to have that surge capacity on the global scale.

Mr. GUEST. As it relates to the National Computer Forensics Institute, do you feel that it serves as a key component in our fight against cyber crime?

Mr. SHERIDAN. Sir, I could not agree with you more wholeheartedly on that question. It trains, equips State, local officers to be the first line of defense, the first people that your constituents are primarily going to call.

With their support—as I mentioned, partnerships in the Secret Service—and shoulder-to-shoulder with us, this is how we are going to beat this adversary and how we are going to get more competent at combating these types of fraud schemes.

Mr. GUEST. As I understand your testimony, Director Sheridan, you believe it is crucial that Congress not only reauthorize this pro-

gram but that we robustly fund what is going on there at the National Computer Forensics Institute. Is that correct?

Mr. SHERIDAN. Yes, sir. I think that is imperative in this fight.

Mr. GUEST. Thank you, Madam Chairman. I yield back.

Ms. SLOTKIN. Perfect timing.

The Chair recognizes for 5 minutes the gentleman from California, Mr. Swalwell.

Mr. SWALWELL. Thank you. I thank the Chairwoman for holding this critical hearing as the dashboard is blinking for America's businesses as it relates to ransomware attacks.

In many ways, this feels like a pre-September 11 environment for businesses, in that you have all the signs there that, you know, we are going to continue to face attacks, perhaps ones that could shut down for a protracted period of time critical infrastructure. You have these attacks being launched from foreign countries that are not our allies. It is unclear whether they are state-sponsored, but they are certainly state-enabled, because countries are looking the other way and aren't cooperating with us or INTERPOL in apprehending and stopping the hackers.

So I wanted to first invoke a Bay Area business leader, John Chambers, who used to be the CEO at Cisco. He recently said that more than 65,000 ransomware attacks are expected to happen this year, at an average cost to small and medium-size businesses of $170,000 each.

Kevin Mandia, the CEO of FireEye, recently said, "There is a direct correlation between ransomware and the anonymity of digital currency." While I certainly am a supporter of cryptocurrency and blockchain technologies, I want to make sure that they are not contributing to or enabling these attacks.

So the question I have first: Is anonymous cryptocurrency hindering your office's abilities at DHS to respond to cyber attacks? Mr. Eisert.

Mr. EISERT. Thank you for that question. To get to your point about the use of virtual currencies in ransomware, the biggest hurdle is already taken care of with those illicit actors. The payer is on-ramping that money into the system for him. That is usually where we have our greatest success, as I discussed before.

As for the fight against network intrusion, H&I has the Cyber Crimes Center, which supports cyber-enabled crimes as well as cyber crime directly. Within the Cyber Crimes Center, we have a network intrusion program; we call it Operation Cyber Centurion. What Cyber Centurion does is, we have trained special agents around the country with specific software and tools, and we scan and detect vulnerabilities in the infrastructure.

So we will scan the open net for vulnerabilities that have been published by our sister agency, CISA, where, when we identify those vulnerabilities, we will reach out to those organizations and say, "Hey, you have a gap here," or, "Hey, you have a gap inside your system right now," and then we will proactively do an investigation with that.

Mr. SWALWELL. Thank you, Mr. Eisert.

To follow up on that, how much does it help when a business reports to you that they have been attacked? How does that factor into whether you think we should have mandatory reporting,

whether it is in critical infrastructure space or just business-wide in America? What information do you yield when you learn about a ransomware attack?

Mr. EISERT. The more dots we have out there, the more connections we can make. So, with the increased reporting, either it be from the financial arena or just in the trend of money laundering and everything else, or private industry on how they have been hacked, when we have more bits of evidence and information, we can connect to bigger networks. So it would be extreme help to have that information.

Mr. SWALWELL. I know there is a lot that we can do, you know, left of boom, as far as, like, the hygiene requirements that we have, particularly of, you know, U.S. Government vendors and contractors. But on the right-of-boom side, what are you doing to make sure that businesses are comfortable working with DHS or the Bureau?

You know, the concern I have heard from some vendors is, you know, we don't want to open our books up to the FBI or DHS; you know, who knows what we have done inadvertently that could put us, you know, on their radar. We don't want them thinking that way. We want them to trust the Government, that the Government can be a part of understanding the attack and, ideally, have the capability to shut it down.

So what are you doing to try and earn the trust of businesses who are victims?

Mr. EISERT. Again, thank you for that question.

Well, we partner tremendously with our brothers and sisters in FBI and CISA in this world. We do a lot of outreach. I spoke earlier about Operation Cornerstone, which does a lot of outreach to private industries to let them know who we are, what we can do, how we can help. With that comes a level of comfortability.

I can't speak for the other agencies on what they do independently, but I think it is important that we continue to work together and show that we are in this with one fight.

Mr. SWALWELL. Great. Thank you.

Thank the Chair for the hearing. I yield back.

Ms. SLOTKIN. Thank you.

The Chair recognizes for 5 minutes the gentleman from the greatest State in the Union, Michigan, Mr. Meijer.

Mr. MEIJER. Amen. Thank you, Madam Chair.

Then thank you to our witnesses for testifying here today and sharing a little bit more of your knowledge and experience and understanding on this critical issue that has obviously been in the news because of ransomware but has been an issue more broadly.

As Ranking Member of this committee's Oversight Subcommittee, I always want to make sure that our Government is functioning as efficiently and as adequately as possible so that we can be most effective in combating terrorism.

You know, we have before us three different subcomponents of the Department of Homeland Security represented. So I will allow whoever feels most well-equipped to answer this question to do so.

But I want to understand, with all of the different Federal entities engaged in countering terrorism financing and the illicit financial activities that help contribute toward it, can you provide a lit-

tle bit more clarity on which specific agencies are responsible for tracking which activities? So what are the left and right limits not only of your own entities but also how you engage with the broader intelligence and law enforcement community in these efforts?

Mr. SHERIDAN. Sir, if I could, I will start conceptually first.

We do recognize the fact that there are certainly overlapping authorities, to some extent, and responsibilities. But we in law enforcement view it as a team sport. There is more than enough work to go around. It is essential that we have that level of partnership and collaboration due to the complexity and the scope and scale of our adversary.

We have institutional deconfliction and information-sharing mechanisms in place to ensure we aren't being wasteful in any way and being good stewards of the American taxpayer dollar, to your concern.

More on a tactical approach, I will speak for the Secret Service, in that our role is focused on protecting the Nation's financial infrastructure and financial payment systems, so we will investigate crimes that violate U.S. law related to those.

Because of those information-sharing mechanisms we have in place through our task forces, with my colleagues here at the table, as well as all of Federal and State and local law enforcement, we are able to share information and case coordination as an investigation comes up that may not focus on those payment systems.

Mr. EISERT. If I may add to that, primacy within the Joint Terrorism Task Force lays with the FBI. So they will always have primacy when it comes to terrorism and terrorism financing. But, like my colleague said, a lot of us bring unique authorities to the table.

H&I is the largest Federal contributor to the FBI's Joint Terrorism Task Force. It speaks specifically about those authorities. Fifty percent, almost 50 percent, of all disruptions within the Joint Terrorism Task Force fall within the authorities that HSI bring to the table—so, for instance, the UC activity, the undercover activity, that we have; full use of Bank Secrecy Act data that we have; full access to trade data.

So each agency is bringing their particular skill set.

Ms. DOBITSCH. I will just add as well, I think, from the intelligence perspective, I&A is really serving as the bridge between the intelligence community and our State and local law enforcement partners.

The first step really is access to that data, making sure that everyone involved in this fight has access to that data and that it is integrated in a way that we could use technology to quickly identify those threats.

We think it is critical—particularly as we talked about how big cryptocurrency is and the use of digital currencies, it requires a sophisticated understanding and expertise but technology to be able to quickly comb through the data and figure out what we should be looking at. So it is really the access and the integration that is critical.

Oftentimes we have local law enforcement information that is filling intelligence gaps and intelligence information that is helping local law enforcement understand what those vulnerabilities are.

Mr. MEIJER. Thank you all for your responses to that to better help, kind-of, flesh out that universe from a top-down level. I am heartened to hear on both the access side and the information-sharing side and on the deconfliction-mechanism side that those have been adequately addressed.

I guess, when it comes to resources and capabilities—and then my time is running short here, but are there any concerns that there may be either gaps in enforcement, gaps in collection, or gaps in capabilities that we should be working to address?

Mr. EISERT. Specific to the virtual currency problem set, the current regulations doesn't encapsulate the whole virtual currency. Virtual currency AML and know-your-customer stuff does not mirror traditional banking industry AML.

Mr. MEIJER. Then, with that, Madam Chair, my time has expired, and I yield back.

Ms. SLOTKIN. Thank you.

I will just note for the Members that we will do a quick second round here.

But the Chair recognizes for 5 minutes the gentleman from New Jersey, Mr. Gottheimer.

Mr. GOTTHEIMER. Thank you, Chairwoman Slotkin, for organizing this very important hearing.

Thank you to each of the witnesses for being here today and for the work you and your colleagues do to help counter the illicit use of cryptocurrencies.

I am concerned about the increasing attractiveness of cryptocurrencies to two types of illicit actors: One, foreign terrorist organizations such as Hamas, Hezbollah, and ISIS, and, second, to the use of domestic White supremacists like the Proud Boys and other violent extremist groups which were involved in the January 6 attack on the Capitol.

If it is OK, I will start with you, Ms. Dobitsch. How does our ability to pursue the illicit use of cryptocurrencies differ between these two types of actors? Is it easier to shut down, seize the assets of, and bring charges against foreign terrorist organizations compared to domestic violent extremists?

Ms. DOBITSCH. Thank you, sir.

I would say that it is complex from both perspectives, in part because of the anonymity that cryptocurrency and other digital currencies provide. Even if we can see the transaction, we often don't know who the transaction—or who is receiving that and then what the ultimate purpose of that resource is.

So it is difficult even from a foreign terrorist perspective to be able to track that money as it relates to it ultimately resulting in the purchase of a weapon or some kind of facilitation of an operation.

From the domestic violent extremist angle, certainly we are seeing an increase in calls for fundraising and donations using cryptocurrency, but we have a difficult time really trying to translate that to violence and understanding how that resource is being translated into a plot or an operation here in the homeland.

Mr. GOTTHEIMER. Thank you. But, compared to cash, is it easier to track, or it is still more difficult because you can't really understand the purpose of it?

Ms. DOBITSCH. I would defer to my law enforcement colleagues on which one is more or less——

Mr. GOTTHEIMER. I guess I will turn to Mr. Eisert on that one, or Mr. Sheridan I guess. I don't know. Who do you think is better on that one?

Mr. SHERIDAN. Is your question about——

Mr. GOTTHEIMER. I guess it is a Secret Service question, so cash——

Mr. SHERIDAN. Is your question about tracking, sir?

Mr. GOTTHEIMER. Yes.

Mr. SHERIDAN. By its nature, digital money is easier to track, because there is a digital trail and actual evidence related to its use and each step it takes along the blockchain as it moves.

Mr. GOTTHEIMER. If I can stick with you, if that is OK, how can we eliminate barriers and friction for law enforcement to make it easier for us to keep up with ever-evolving digital assets and technologies? Is there anything you think we should be doing straightaway?

Mr. SHERIDAN. For us, it would be resourcing in the basic concepts of people, process, and technology.

We need to increase our work force, not only in volume but in capabilities, on the law enforcement side as well as the subject-matter experts, our professional work staff that we hire. We have a great team of computer scientists, folks with the capabilities to conduct blockchain analysis and crypto tracing, but we need more of them.

We need to keep pace with the adversary. We need to grow into the international locations where we don't have as strong a presence, because this is a transnational crime.

We need to get better at our processes, to modernize and have more advanced capabilities to handle the volume of data that we are seeing, because there is such a significant trading and movement related to these currencies.

We also need to modernize our technologies related to our task forces throughout the globe.

Mr. GOTTHEIMER. Thank you, sir.

Mr. Eisert, would you describe the role undercover HSI agents placed in last year's seizure of millions of dollars in cryptocurrencies from terrorists, including ISIS, al-Qaeda, and Hamas, if you don't mind? Thanks.

Mr. EISERT. Absolutely. Excuse me, though, if I stay vague. There is a lot of undercover activity and Classified information that we are happy to host a separate meeting on.

Mr. GOTTHEIMER. Of course.

Mr. EISERT. But those initial leads, if I can just bulk them together—they ran parallel and were very similar—those initial leads came through the Intelligence Committee as well as some reporting from watchdog organizations.

Upon identifying the illicit intent of those organizations, we approached each of those organizations with multiple undercover personas, engaged them in conversation to get the intent of what the purpose of the money was, at which point we started to identify the Bitcoin wallets that they asked for.

Throughout the investigation, their methods changed, but with each method change we just identified a new branch of tracing that we had to run and go do, bringing it right to the end, bringing it right to the culmination of the seizure of about $10 million in both cases.

Mr. GOTTHEIMER. Excellent. I appreciate that. I would enjoy a briefing in a Classified setting on that.

Mr. EISERT. Excellent.

Mr. GOTTHEIMER. Thank you so much.

I yield back. Thank you, Chairwoman.

Ms. SLOTKIN. Thank you.

We will now turn to a second round. I will recognize myself for some questions.

So two very different questions. One is on this idea that our companies, our organizations, even local governments are not mandated reporters when it comes to the attacks that they withstand.

So, for instance, a big box store could be hacked and have a ton of all of our personal data taken and then pay a ransom for that money, potentially through cryptocurrency, and not have to report that to the very individuals who had their information stolen, not have to report that to law enforcement, not have to actually say anything. We have seen examples of companies who have waited 6 months, a year, et cetera, to actually come forward and say something about this.

Tell me, for the folks in law enforcement, what that does to your ability to actually help go after these guys. Do you believe that companies and organizations should be mandated reporters when they are the victim of a hacking or ransomware attack?

Mr. Sheridan.

Mr. SHERIDAN. Thank you, ma'am. That is an extremely important question. We, yes, support reporting in all instances to law enforcement, regardless of agency or which law enforcement entity it is reported to.

I do believe there are some misconceptions about law enforcement's role in this, as was referenced earlier, that perhaps law enforcement creates an intrusion or creates some type of vulnerability to systems.

We view our investigative mission as part of the prevention process. We will work with organizations and whatever third party they have as part of their security team in a collaborative sense.

Reporting to us will help make systems stronger, will help identify areas of weakness, the attack vectors, the indicators of compromise. It will prevent future attacks not only to that individual organization but perhaps other organizations that may have similar vulnerabilities.

Ms. SLOTKIN. Yes.

You know, I talk to people in my district, and they feel like their data, their information, they are on the front lines of, kind-of, a cyber war. They are asking me constantly, you know, are we doing something about this? Is my Government helping to stop these attacks?

A lot of people took notice when the Colonial Pipeline was attacked and ransomed, when, you know, we got money back through the FBI acting to grab some of that money back. It felt like the

first time we were punching back—in a public way, right? Of course, there are lots of that things I know you can't talk about that, and we are glad to not talk about them.

But help explain to, again, that farmer in the middle of my district who is asking about cybersecurity. Convince him that their Government is doing something about the fact that they are being constantly attacked.

Mr. SHERIDAN. Yes, ma'am.

Well, it starts, as was referenced earlier, with the National Computer Forensics Institute. We have trained over 16,000 State and local officers to be the first responders to these events. It starts with contacting them, contacting law enforcement.

There are multiple tools within our organizations and our partners in order to interdict and stop in real time some of these victimizations that are occurring, not only within the network itself but in terms of the transfer of the funds that have been taken by these illicit actors.

Within the Secret Service, we have our Global Rapid Response and Incident Tracking Team that is able to domestically stop wire transfers if notified within a certain amount of time. Since its inception in——

Ms. SLOTKIN. If notified. Uh-huh.

Mr. SHERIDAN. If notified.

Ms. SLOTKIN. Right.

Mr. SHERIDAN. If it is notified, since 2019, we have intercepted more than $80 million in transit to prevent it from going to illicit actors.

Within the Department of Treasury, FinCEN has their Rapid Response Program. Similarly, that is more internationally focused, but, over the past 4 years, we have an 82 percent success rate working with FinCEN if notified within a 72-hour window, primarily within a 48-hour window. The success rate drops dramatically depending on the amount of time that has lapsed. But we have been able to interdict more than $385 million from going to criminal actors.

Within the Secret Service, we have our own Asset Forfeiture Branch that returns victim funds to victims if we are notified, if we are able to participate in the investigation and find the illicit funds in transit.

Ms. SLOTKIN. So that is super-helpful and connects the two questions, right, that you all can actually do some real things if you are notified, but our current system does not require organizations or companies to notify anybody if their data has been taken, if there has been ransom.

So I appreciate that and would offer that we could do with a little bit more public talk and discussion from you all about what you are doing, because it sounds like it is more than the average citizen knows, and they want to know that their Government is protecting them.

So, with that, I yield to the gentleman from Texas, Mr. Pfluger.

Mr. PFLUGER. Thank you, Madam Chair.

Kind-of discussing a similar topic, you know, attribution seems to be one of the toughest things to get after. So, whether it is mandatory or whether this public-private partnership encourages peo-

ple because they know that, if the assets that they have potentially lost are going to be returned to them, then hopefully that will also drive a motivation to report—and especially if the education is out there and we have forums where they understand that, you know, your agencies offer them something to prevent this type of activity from happening.

But let me kind-of focus in on the National Computer Forensics Institute and why it is valuable to the Secret Service in your investigations and what more it can be doing and how can we in Congress support you.

Mr. Sheridan.

Mr. SHERIDAN. Yes, sir. Thank you for the question.

We are very, very grateful for Congress's support to this date regarding NCFI. It has been phenomenal to see the growth in that program and the number of people and State and local officers, judges, and prosecutors that have been trained there, over 16,000 to date.

We are currently training about 3,000 a year. Projected estimates are almost twice that, but we are limited by not only the authorization that is pending in 2022 to sunset but the current resourcing that we have to that facility.

We think we can double our capacity in terms of training, as well as expand into international areas, which I think is imperative for us to be stronger globally with our law enforcement partners around the world in order to combat this.

Mr. PFLUGER. Well, thank you.

Just a question for any of you that wants to comment on this. How closely linked are terrorist organizations and these ransomware attacks that we are seeing, which are not new, but some of them are being publicized, especially the ones that are happening toward critical infrastructure, whether it is our food supply, our energy supply? How closely linked, and what is the projected or estimated threat, as you see it with your crystal ball, in the future?

Ms. DOBITSCH. So, to date, we haven't seen really any connections between ransomware attacks and terrorist groups or associates.

But what we would underscore is, as we discussed earlier, that rapid ability to adapt that we have seen demonstrated by the broad range of terrorist groups. In addition to that, we call it the copycat trend. Terrorist groups often adopt tactics, techniques, and procedures from other malicious actors that they see as beneficial to them.

So, again, as terrorists' use of cryptocurrency and digital currencies becomes more commonplace, certainly we could expect to see them using ransomware as a means to fund their operations.

In addition to that, we are increasingly seeing cyber criminals offer ransomware as a service. So individuals can buy a service on the dark web, and we often don't know who the actor is that is paying for that service.

So there are many opportunities for terrorists to exploit ransomware to support their operations.

Mr. PFLUGER. Again, probably underscoring the NCFI, your role that you play there.

I would just say, based on that response, that I don't think—our position on this has to be incredibly strong. The responses that we as a country levy upon bad actors, criminal organizations, terrorist organizations, malign actors anywhere, state or non-state—it is not limited to 16 industries in this country; it is going to be across the board. Our response has got to be strong. I hope that this committee will continue to take that up and investigate this.

With that, Madam Chair, I will yield back.

Ms. SLOTKIN. The Chair recognizes the gentleman from New Jersey, Mr. Malinowski.

Mr. MALINOWSKI. Thank you, Madam Chair.

So I am still not convinced this market in cryptocurrency should even exist, but let's talk about regulation for a moment.

The Treasury Department recently announced that it would be requiring cryptocurrency transactions I believe over $10,000 to be reported to the IRS. Is that correct?

Mr. EISERT. I believe there is proposed legislation.

Mr. MALINOWSKI. It is proposed, right. So that does require action from us? Or is this something that——

Mr. EISERT. I would have to defer to Treasury on that.

Mr. MALINOWSKI. OK.

In principle, would that at least help to address the challenge that Chairwoman Slotkin referred to, in the sense that presumably a company making a ransom payment of over $10,000 would then at least have to report that to the IRS?

Mr. EISERT. I would say depending on how the regulation is written.

Mr. MALINOWSKI. Right.

Mr. EISERT. If we want to take mainstream financial institutions and how regulations are written now, if cash was to go into the system, there would be a requirement. Right now, the mainstream regulation revolves around cash.

Mr. MALINOWSKI. OK.

Mr. EISERT. If it mirrored it with virtual currency, then yes.

Mr. MALINOWSKI. That would presumably be helpful to you all.

Mr. EISERT. Extremely.

Mr. MALINOWSKI. Yes. OK. Most ransomware payments would be over $10,000, just in the current scheme of things, so it would probably capture a significant share of, if not all, ransomware payments.

Other ideas? Should the SEC be given the authority to regulate cryptocurrency exchanges? Is that something that the administration is considering proposing?

Mr. SHERIDAN. So, sir, the challenge with regulation that we see is, because digital money is used in so many different capacities, depending on the technology that is used to create it and, essentially, how it is employed, there is no one regulatory agency that currently has oversight. Sometimes it is a commodity, sometimes it is a security, a derivative, legal tender.

So regulation is certainly important, as my colleague has identified. The anti-money-laundering laws, know-your-customer, countering of financing of terrorism, the anti-money-laundering law of 2020 have all been instrumental in helping tamp down criminal activity related to this. But, from a law enforcement perspective, we

are not regulatory in nature, and our perspective would be to grow authorities related to our investigative and statutory capabilities as opposed to regulatory capabilities.

There is some concern, as also was referenced, about the dual-edged nature of overregulation that may push illicit use and criminal actors deeper into anonymizing methods and corners of the internet that would make it more difficult for law enforcement.

Mr. MALINOWSKI. OK. Well, you know, we would very much value, I think, your guidance in finding that sweet spot, if the answer is going to be greater regulation.

I presume that you would agree that, whatever rules we come up with, they should be broadly harmonized across the 50 States but also internationally. I wonder if you know of any examples outside the United States of regulatory steps that other governments, partner governments, have taken that you think might be helpful to emulate or, on the contrary, helpful not to emulate.

Mr. EISERT. Sure. Thank you.

Homeland Security Investigations sits on working groups with the Financial Action Task Force, FATFs, which is a conglomerate of countries and regulatory bodies. In this working group, we discuss those exact things—where should we be going? Many of the regulations you are seeing proposed and that have already come through are a result of those FATFs.

You know, with that, the regulations and know-your-customer, they are meant to root out bad actors, support OFAC fundings. At no point do they restrict legal transfer of these virtual currencies. So it is important to note that, no matter what has been proposed, nothing is restricting the use of virtual currency. It is just creating obtainable records to root out the bad actors.

Mr. MALINOWSKI. OK. Thank you.

I yield back.

Ms. SLOTKIN. The Chair recognizes the gentleman from Michigan, Mr. Meijer.

Mr. MEIJER. Thank you, Madam Chair.

I just want to follow up on the earlier line of questioning that I had. Mr. Eisert, I think you mentioned that one of the—you know, the gaps that you identify when it comes to specific and virtual currency problem sets. We have been talking about that a little bit.

I want to drill down, because I think many who are watching or listening here today are familiar with Bitcoin. They have at least heard of Bitcoin, if they are not more broadly aware of blockchain and crypto. But Bitcoin, though it is the most well-known and one of the largest by market—or the largest by market capitalization, it is one of, I think, over 5,000 different cryptocurrencies. So you have not only, you know, some others that people may have heard of, like Litecoin, Ethereum, Doge, but also many, many, many old coins and then proposed stable coins as well.

Ms. Dobitsch, in your report, you also said—or your testimony, you also said that newer and less popular cryptocurrencies are increasingly attractive to malicious actors because of their more stringent privacy and security features.

I guess, how well-resourced do you feel to deal with the lesser-known cryptos, not just those who may be in the top, you know,

5 or 10 of market cap, but even the potential for the exploitation of some of these mini or micro cap cryptocurrencies?

Mr. EISERT. The privacy coins create a challenge because of their hidden blockchain, their obscured blockchain. A lot of our data analytics aren't as thorough as it is with the open blockchains, and sometimes it is not thorough enough for us to bring it to a courtroom to do something.

Luckily for us, because, as you mentioned, the market cap and the total volume of coin, the usability is not there. If you are looking at Monero, with maybe a market cap right now of 40 to 50 million, if you are looking to move 3 million in Monero, you are using 10 percent of the market.

So the usability is not there yet, and that is the scary part. The good thing is a lot of U.S. exchanges will not accept Monero because of its hidden blockchain. It won't meet their know-your-customer and AML policies.

Mr. MEIJER. Well, I actually want to follow up on that point, because, you know, when terrorists were aware that email traffic might be monitored, I mean, the way you get around that is you don't have that go through traffic, right? You have a draft, and then two parties both have access.

I mean, what about a scenario where it is a super-micro-mini cap where it is not usable as a currency but if a company were to invest, you know, $10 million into it and, prior to that investment, a terrorist or ransomware entity, you know, buys up the entirety of it, I mean, it is essentially functioning as a mechanism to pass that through. Because, once the money is in there, they could just sell whatever the gains are, and then, you know, all of the losses are borne by the entity that had purchased—that company paying that ransom.

I mean, that would obviously be a scenario where, to Mr. Malinowski's reference to the proposed Treasury Department regulations, it would not qualify, because it isn't a transfer. It is merely a purchase that is held. But that asset, essentially like a balloon deflating, loses all value, and all the air is captured on the outside.

I mean, is that a scenario you could foresee happening?

Mr. EISERT. Yes, I am trying to track most of it.

Some of the regulations being proposed—and, again, I really would prefer to yield to Treasury on something like that—is, if an unhosted wallet has an exchange with a regulated wallet, there would be a reporting mechanism. So that would capture some of that.

As for an alt-coin or a privacy coin that an organization decides to use and pump a lot of money in, that is great; they are still going to have the problem of—I am going to keep using the term—"off-ramping" it. That is where the AML, the anti-money-laundering, policies will take effect and capture.

Mr. MEIJER. Ms. Dobitsch, anything to add?

Ms. DOBITSCH. No, just that we have seen terrorist groups use privacy coins, including Monero. So it is certainly something that we are seeing.

I would also note that, you know, thousands of cryptocurrencies; the advancements are daily. So the increased privacy, the increased anonymity of these occurs with the creation of every new Bitcoin.

So it is certainly a challenge, I think, first, to understand what they are using and then to have greater insight into how they are actually using the currency.

Mr. MEIJER. OK.

Well, I appreciate the additional ability to probe a little bit deeper there. It is clearly that, you know, Bitcoin presents its own challenges, but, in the broad, you know, ecosphere of various cryptocurrencies, especially when we get down to that very small end, the opportunities for exploitation are nearly limitless.

With that, Madam Chair, my time has expired, and I yield back.

Ms. SLOTKIN. With that, I thank the witnesses for their testimony and the Members for their questions.

The Members of the subcommittee may have additional questions for the witnesses, and we ask that you respond expeditiously in writing to those questions.

The Chair reminds Members that the subcommittee record will remain open for 10 business days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 11:39 a.m., the subcommittee was adjourned.]